

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA  
**UNIVERSIDAD**  
**CATÓLICA**  
DEL PERÚ

### DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UN INSTITUTO EDUCATIVO

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

**Luis Carlos Aliaga Flores**

**ASESOR: Moisés Villena Aguilar**

Lima, Febrero del 2013

## Resumen del proyecto de tesis

En el transcurrir de las últimas décadas, el tema de la seguridad de información se ha convertido en un aspecto vital en la gestión de las organizaciones. Conforme van saliendo a la luz incidentes de seguridad que afectan a grandes empresas internacionalmente reconocidas, la sociedad cada vez más va tomando conciencia de la importancia y el valor que representa la información. Estas incidencias ocurrieron con mayor frecuencia en la década del 2000 con los famosos “Wikileaks”, los cuales, entre otros informes, publicaron diversos documentos de gobiernos de distintos países con contenido muy confidencial.

Frente a esta realidad, se observa que el no contar con un programa de seguridad de información que brinde las garantías necesarias para la información en cualquier organización, en medio de un mercado tan competitivo como el actual, representa una desventaja considerable frente a empresas del mismo rubro que sí trabajan el tema dentro de su cultura organizacional. Esta desventaja podría traer pérdidas muy graves, tales como la pérdida de un número importante de clientes o de acuerdos laborales con otras empresas, lo cual afectaría principalmente la parte financiera de la organización, y finalmente podría, si las pérdidas llegan a ser críticas, llevar a la quiebra al negocio.

En el caso de instituciones educativas, se puede observar que éstas aún no toman a la seguridad de información como prioridad. Así como también se observa que no existe una cultura de seguridad transversal en dichas entidades. Si bien es cierto que aún no existe una regulación del Ministerio de Educación, no se tendría que esperar que el tema se regule para que recién tomar acción en el establecimiento de controles para mitigar o reducir los riesgos a los que la información de estas entidades está expuesta.

Bajo este contexto, el presente proyecto brinda como alternativa el diseño de un Sistema de Seguridad de Información (SGSI) para una institución educativa de nivel superior, tomando la realidad de una entidad educativa local. La presente tesis se enfoca en proteger la información de los procesos principales de esta institución educativa siguiendo normas internacionales vigentes.

## Dedicatoria

A ti mamá, por ser mi ejemplo a seguir, por darme fuerzas cuando flaqueaba y por guiarme con tu luz siempre por el camino correcto. Nunca estaré lo suficiente agradecido con Dios por haberme regalado una madre como tú.

Nada de esto hubiera sido posible sin tu apoyo papá. Estuviste físicamente lejos pero gracias a tus consejos y aliento soy la persona que soy ahora. Estos son los frutos de tu empuje y valentía al emprender la aventura que iniciaste hace más de 10 años atrás.

A Emily, por darme otra visión de las cosas y por apoyarme a que yo cumpla exitosamente los retos de la vida.



## Agradecimientos

Al Ing. Moisés Villena por su valioso apoyo y asesoría en el desarrollo del presente trabajo.

A la Sra. Rosa María Marisca por su valioso apoyo y disposición para el desarrollo del presente trabajo.

Al Ing. Manuel Tupia por enseñarme que no todo en la carrera de Ingeniería Informática es programación. Usted fue el que me inspiró a seguir esta línea de carrera profesional.



## Índice de Contenido

|   |    |
|---|----|
| Capítulo 1: Generalidades .....                                     | 1  |
| 1. Introducción.....  | 1  |
| 2. Definición de la problemática .....                              | 2  |
| 3. Objetivo general .....   | 3  |
| 4. Objetivos específicos.....                                       | 3  |
| 5. Resultados esperados.....  | 3  |
| 6. Alcance y limitaciones .....                                     | 4  |
| 6.1. Alcance .....  | 4  |
| 6.2. Limitaciones .....   | 5  |
| 7. Métodos y procedimientos .....                                   | 5  |
| 7.1. Metodología del producto.....                                  | 5  |
| 7.2. Metodología del proyecto.....                                  | 7  |
| 8. Justificación y viabilidad .....                                 | 7  |
| 9. Plan de proyecto.....  | 9  |
| 9.1. Estructura de Descomposición del Trabajo (WBS).....            | 9  |
| 9.2. Diagrama de Gantt.....   | 10 |
| 10. Marco conceptual .....  | 11 |
| 10.1. Conceptos clave .....   | 11 |
| 10.1.1. Activo.....   | 11 |
| 10.1.1.1. Control.....  | 11 |
| 10.1.1.2. Información.....  | 12 |
| 10.1.1.3. Confidencialidad .....                                    | 12 |
| 10.1.1.4. Disponibilidad.....                                       | 12 |
| 10.1.1.5. Integridad.....   | 12 |
| 10.1.2. Seguridad de Información .....                              | 12 |
| 10.1.2.1. Evento de seguridad de información.....                   | 13 |
| 10.1.2.2. Incidente de seguridad de información .....               | 13 |
| 10.1.3. Sistema de gestión de seguridad de información (SGSI) ..... | 13 |
| 10.1.3.1. Proyecto de SGSI.....                                     | 13 |
| 10.1.4. Amenaza.....  | 13 |

|  |   |    |
|--|---|----|
| 10.1.5.  | Vulnerabilidad .....  | 13 |
| 10.1.6.  | Riesgo .....  | 13 |
| 10.1.6.1.  | Análisis de riesgo .....  | 14 |
| 10.1.6.2.  | Evaluación del riesgo.....  | 14 |
| 10.1.6.3.  | Gestión del riesgo .....  | 14 |
| 10.1.6.4.  | Tratamiento del riesgo.....   | 14 |
| 10.1.6.5.  | Riesgo residual .....   | 14 |
| 10.1.6.6.  | Aceptación del riesgo .....   | 14 |
| 10.1.7.  | Política .....  | 14 |
| 10.2.  | ISO/IEC 27001:2005.....   | 14 |
| 10.3.  | ISO/IEC 27002:2005.....   | 15 |
| 10.4.  | ISO/IEC 27003:2010.....   | 16 |
| 10.5.  | ISO/IEC 27005:2008.....   | 18 |
| 10.6.  | COBIT 5 .....   | 19 |
| 11.  | Revisión del estado del arte .....                                      | 23 |
| 11.1.  | Universidad Nacional de Ciencia y Tecnología de Taiwán.....             | 23 |
| 11.2.  | Universidad Libre de Bozen/Bolzano .....                                | 24 |
| 11.3.  | Universidad Kyushu .....  | 25 |
| 12.  | Discusión sobre los resultados de la revisión del estado del arte ..... | 26 |
| Capítulo 2: Procesos de un instituto educativo ..... |   | 27 |
| 1.   | Modelamiento de los procesos “core” de un instituto educativo.....      | 27 |
| 1.1.   | Proceso de Diseño y Desarrollo de Nuevos Productos .....                | 27 |
| 1.2.   | Procesos de Programación Académica y de Recursos .....                  | 28 |
| 1.2.1.   | Proceso de Programación de Frecuencias .....                            | 28 |
| 1.2.2.   | Proceso de Programación de Facilitadores .....                          | 29 |
| 1.2.3.   | Proceso de Programación de Aulas.....                                   | 30 |
| 1.3.   | Procesos de Captación y Admisión de Alumnos.....                        | 30 |
| 1.3.1.   | Proceso de Organización de Charlas Informativas.....                    | 30 |
| 1.3.2.   | Proceso de Ventas de Carreras.....                                      | 31 |
| 1.4.   | Procesos de Matrícula .....   | 31 |
| 1.4.1.   | Proceso de Admisión y Matricula de Ingresantes .....                    | 32 |
| 1.4.2.   | Proceso de Matricula Secuencial .....                                   | 32 |

|   |    |
|---|----|
| 1.5. Proceso de Titulación .....                            | 32 |
| 2. Identificación de activos .....                          | 34 |
| 3. Valorización de los activos de información .....         | 39 |
| Capítulo 3: Identificación y Evaluación de los Riesgos..... | 46 |
| 1. Mapa de Riesgos .....                                    | 46 |
| 2. Plan de tratamiento de riesgos .....                     | 56 |
| 3. Controles para el tratamiento de riesgos.....            | 56 |
| 4. Mapeo de los controles con COBIT 5 .....                 | 65 |
| Capítulo 4: Entregables de un SGSI .....                    | 76 |
| 1. Declaración de la Aplicabilidad .....                    | 76 |
| Capítulo 5: Conclusiones y recomendaciones .....            | 82 |
| 1. Conclusiones y observaciones.....                        | 82 |
| 2. Recomendaciones .....                                    | 83 |
| Bibliografía .....  | 85 |

## Índice de Figuras

|   |    |
|---|----|
| Figura 1. Modelo PDCA aplicado a un SGSI.....                               | 6  |
| Figura 2. EDT del proyecto .....  | 9  |
| Figura 3. Diagrama de Gantt del proyecto .....                              | 10 |
| Figura 4. Modelo PDCA aplicado los procesos ISO/IEC 27001 .....             | 15 |
| Figura 5. Secciones del ISO/IEC 27002.....                                  | 16 |
| Figura 6. Fases del proyecto de SGSI .....                                  | 17 |
| Figura 7. Proceso de la gestión de riesgos de seguridad de información..... | 19 |
| Figura 8. Los cinco principios del marco COBIT 5 .....                      | 21 |
| Figura 9. Los siete habilitadores del marco COBIT 5 .....                   | 22 |
| Figura 10. La cascada de objetivos de COBIT 5.....                          | 23 |





## Índice de Tablas

|   |    |
|---|----|
| Tabla 1. Inventario de activos .....  | 34 |
| Tabla 2. Criterios de valorización de activos .....   | 39 |
| Tabla 3. Valores según nivel de criticidad .....  | 40 |
| Tabla 4. Valorización de los activos .....  | 41 |
| Tabla 5. Matriz de calor .....  | 47 |
| Tabla 6. Descripción de los niveles de la Probabilidad de Afectación .....                          | 47 |
| Tabla 7. Descripción de los niveles de Impacto en el Negocio.....                                   | 47 |
| Tabla 8. Matriz de riesgos .....  | 48 |
| Tabla 9. Plan de tratamiento de riesgos.....  | 56 |
| Tabla 10. Políticas de seguridad .....  | 57 |
| Tabla 11. Controles para el tratamiento de riesgos .....  | 59 |
| Tabla 12. Objetivos organizacionales de la entidad educativa según COBIT 5.....                     | 65 |
| Tabla 13. Objetivos de TI de la entidad educativa según los objetivos organizacionales .....        | 66 |
| Tabla 14. Procesos habilitadores de COBIT 5 según los objetivos de TI de la entidad educativa ..... | 69 |
| Tabla 15. Procesos habilitadores de COBIT 5 para la entidad educativa.....                          | 70 |
| Tabla 16. Declaración de la Aplicabilidad .....   | 76 |

## Capítulo 1: Generalidades

### 1. Introducción

En este capítulo se analizará sobre el contexto actual en el que la seguridad de información se encuentra, en conjunto con el objetivo general, objetivos específicos y los resultados esperados que se tendrían con la finalización del presente proyecto de tesis. Asimismo, se determinara el alcance y las limitaciones que el SGSI tendrá dentro de la institución educativa de nivel superior, en conjunto con la metodología que se seguirá para el desarrollo de proyecto y de producto. Finalmente, se especificara la razón por la que el diseño de un SGSI es la solución frente a la problemática actual y se mostrará el plan del proyecto que se seguirá durante el diseño del SGSI en el instituto educativo, de tal manera de concluir con el presente tema de tesis durante los plazos de tiempo establecidos.

Los puntos a tratar en este capítulo serán:

- Problemática de la seguridad de información en la actualidad.
- Objetivo general de la tesis.
- Objetivos específicos y los resultados esperados de cada objetivo.
- Alcance de la tesis.
- Limitaciones que se encontraron en la elaboración del diseño del SGSI.
- Metodología del producto y del proyecto de tesis.

- Justificación de un SGSI.
- Estructura de descomposición del trabajo de tesis y el plan del proyecto de tesis.
- Marco conceptual y estado del arte.

## 2. Definición de la problemática

Hoy en día vivimos en una sociedad donde uno de los principales activos de cualquier organización o empresa es la información, no importando su tamaño o giro del negocio. Si ocurriera algún incidente relacionado a la integridad, disponibilidad o confidencialidad a la información de cualquier empresa, podrían generarse desventajas competitivas importantes con respecto a otras empresas del mismo sector e incluso podría dejarla expuesta a la quiebra.

En conjunto con el factor humano, la tecnología permite gestionar y manejar la información de las organizaciones. A medida que esta tecnología vaya avanzando, de la misma manera se deberá alinear y sincronizar cada vez más a los objetivos y procesos de negocio como soporte para su respectivo cumplimiento. Actualmente, se puede apreciar que las empresas han automatizado casi todos los procesos de negocio mediante algún software o uso de tecnología.

Como resultado del incremento de la dependencia de las organizaciones respecto a la tecnología para el manejo de su información y del incremento de interconectividad en el ambiente comercial, la información cada vez está más expuesta a una variedad más amplia y sofisticada de amenazas y vulnerabilidades. Estas amenazas pueden ser internas, externas, premeditadas, accidentales, etc. En la mayoría de los casos mencionados, se generan diversas pérdidas dentro de la organización, siendo las reputacionales las más difíciles de contrarrestar.

Por tanto, deberían aplicarse marcos y políticas de control implementadas dentro de una organización para minimizar los riesgos y asegurar la continuidad del negocio. En algunos sectores de la industria, existen entes reguladores que establecen normas obligatorias y recomendadas con respecto a dichos marcos y políticas de la seguridad de información. Sin embargo, en el sector educativo no existen leyes o normas establecidas por parte del Ministerio de Educación que regulen la seguridad de información dentro de las organizaciones bajo su jurisdicción. En consecuencia, se genera una falta de conocimiento e interés de dicho tema en las instituciones educativas

En muchos casos, la razón por la cual estas instituciones educativas no han implementado estas políticas de seguridad de información es porque aún no han tenido algún incidente de seguridad relativamente grave, lo cual comprueba que las entidades peruanas siguen siendo reaccionarias y no preventivas, o asumen que es un gasto que

no retornara las inversiones de dichas políticas, no siendo ningún instituto educativo hasta la fecha la excepción a dichas instituciones educativas a nivel superior.

Dentro del contexto presentado, se propone el desarrollo de un sistema de gestión de seguridad de información (llamado por sus siglas SGSI), el cual permitirá proteger los activos de información y la información que se manejen dentro del flujo de los procesos más importantes en una institución educativa de nivel superior.

### 3. Objetivo general

El objetivo de este proyecto es diseñar un Sistema de Gestión de Seguridad de Información (SGSI) basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios la actual versión de COBIT.

### 4. Objetivos específicos

- i. Modelar los procesos de negocio que componen el alcance del SGSI establecido por la entidad.
- ii. Identificar y valorar los activos de información asociados a los procesos de negocios establecidos como alcance del SGSI.
- iii. Identificar, analizar y evaluar los riesgos a los que están expuestos los activos de mayor valor para la entidad.
- iv. Seleccionar los controles que permitan gestionar y tratar los riesgos identificados.
- v. Formalizar la declaración de la aplicabilidad del SGSI.
- vi. Elaborar la documentación exigida por la norma internacional adoptada para el diseño del SGSI.

### 5. Resultados esperados

- i. Modelamiento de los procesos de negocio que componen el alcance de la presente tesis.
- ii. Inventario de los activos de información críticos del instituto educativo relacionados a los procesos de negocios del alcance del SGSI.
- iii. Mapa de los riesgos de la seguridad de información a los que los activos críticos identificados están expuestos.

- iv. Lista de controles que permitan gestionar los riesgos identificados en los activos críticos del instituto educativo.
- v. Declaración de la aplicabilidad (SoA) para el SGSI.
- vi. Documentación solicitada por la norma ISO 27001 para el SGSI.

## 6. Alcance y limitaciones

### 6.1. Alcance

El alcance del presente proyecto de diseño de un SGSI para entidades educativas de nivel superior/técnico ayudará a alcanzar los objetivos de negocio de la institución educativa estudiada, identificados en las primeras reuniones con la alta gerencia. Estos son:

- Incremento en la retención de alumnos como resultado de la mejora de la calidad y la consolidación del modelo educativo de formación emprendedora.
- Carrera de “Administración de Negocios” acreditada internacionalmente e iniciada la acreditación nacional.
- Presencia de la institución educativa fortalecida a nivel nacional con una oferta diversificada y una mayor captación de alumnos en todos los programas académicos que la institución ofrece.
- Proceso de virtualización de la oferta de la institución educativa iniciado.
- Incremento en la productividad del equipo que integran de la institución educativa.

Este instituto maneja una división de procesos que comprenden los estratégicos, los operativos y los de soporte.

El Sistema de Gestión de Seguridad de Información (SGSI) se diseñará teniendo como base los procesos que la organización considera como “core” del negocio. Estos se encuentran dentro de la familia de procesos operativos.

Los procesos que se encuentran dentro de la familia de procesos operativos son:

- Diseño y desarrollo de los programas académicos.
- Programación académica y de recursos.
- Captación y admisión de alumnos.
- Matricula.
- Enseñanza-Aprendizaje.
- Titulación y certificación.

Todos los procesos mencionados tienen como el proceso de la “Gestión de la calidad educativa” como transversal a la organización. Asimismo, cabe resaltar que el proceso de “Enseñanza y Aprendizaje” es un proceso que no implica tareas o actividades por parte del personal administrativo y académico ya que se enfoca en la enseñanza del día-a-día de los alumnos. Este es el principal motivo por el que no se tomará en cuenta en el alcance del presente proyecto.

## 6.2. Limitaciones

- a) La falta de disponibilidad de la Alta Gerencia, principalmente de la persona responsable del área de TI en el instituto educativo.
- b) Falta de un oficial de seguridad de información dentro de la institución educativa para que apoye y de soporte al diseño del proyecto. El área encargada del tema de la seguridad de información es el área de TI, no siendo su principal prioridad actualmente.

## 7. Métodos y procedimientos

### 7.1. Metodología del producto

Para el diseño de un SGSI, la norma ISO 27001 adopta el ciclo de Deming como metodología, el cual se puede aplicar a todos los procesos que abarca el SGSI. Dicha metodología es más conocida por sus siglas en inglés como PDCA: Plan-Do-Check-Act.

El concepto del PDCA nació a finales de la década de 1970 y fue propuesta por Edwards Deming, quien es considerado por muchos como el precursor del control de la calidad moderno. Dicho concepto nació del método científico: las etapas de hipótesis, experimentación y evaluación del método científico, se relacionan a Plan, Do, y Check del ciclo de Deming. [5]

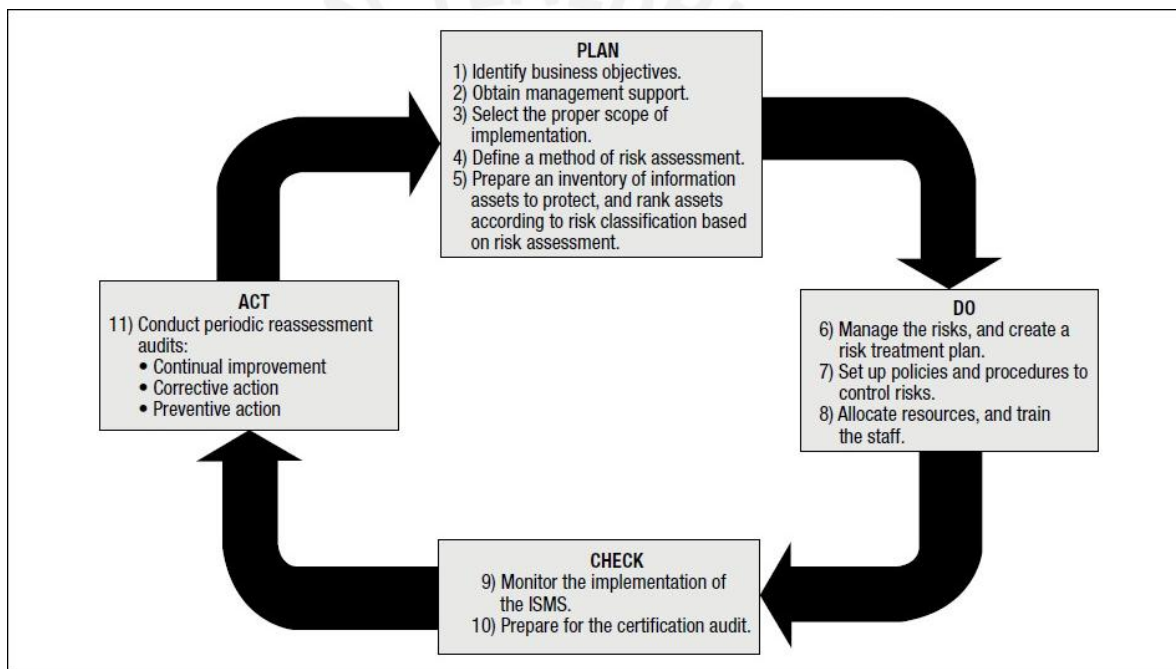
A continuación, se explicaran brevemente los pasos que se siguen en el ciclo de Deming:

- Plan: Se establecen las actividades y procesos necesarios para alcanzar los resultados esperados establecidos por la(s) parte(s) interesada(s).
- Do: Se implementa el plan establecido, se ejecuta los procesos estudiados y, finalmente, se empieza a desarrollar el producto.



- Check: Se estudia los resultados luego de ejecutar los procesos y actividades mencionados en el “Do” y los compara con los resultados esperados del “Plan” para analizar posibles diferencias.
- Act: Se realiza acciones correctivas para alcanzar los resultados esperados si es que hubiera alguna diferencia con los resultados obtenidos.

Esta metodología PDCA es la que se usa como metodología del producto para este proyecto. Dicho ciclo no solo ayuda a alcanzar los objetivos específicos, sino además a conseguir los resultados esperados mencionados anteriormente. Además que es fuertemente recomendada por la ISO y es la metodología más usada para este tipo de proyectos. La figura 1 nos da un panorama de cómo se adapta el ciclo de Deming para el diseño, implementación y monitoreo de un SGSI.



**Figura 1. Modelo PDCA aplicado a un SGSI [5]**

Este proyecto abarcará la fase del Plan del ciclo PDCA, de acuerdo a dos etapas:

- Para la primera etapa, se identificaron los objetivos de negocio de la institución educativa; se determinó el alcance apropiado que tendrá el SGSI en la empresa; se identificaron y analizaron los activos que están involucrados en el alcance del SGSI; se definió una metodología de evaluación de riesgos y se determinó que activos de información están sujetas a riesgos.

- En la segunda etapa, se determinó el plan de tratamiento de los riesgos encontrados y, finalmente, se elaboró las políticas y procedimientos para el control de dichos riesgos y la declaración de aplicabilidad.

## 7.2. Metodología del proyecto

La metodología para gestionar la tesis como proyecto que se seguirá es la establecida por el Project Management Institute en su libro PMBOK.

La guía del PMBOK fue distribuida en el año 1987, en un intento del PMI para documentar y estandarizar información y prácticas generalmente aceptadas en la gestión de proyectos. Actualmente, dicha guía es internacionalmente aceptada y reconocida en la profesión de la dirección de proyectos.

El PMBOK reconoce cinco grupos de procesos básicos y nueve áreas de conocimiento comunes a casi todos los proyectos. Estos procesos son: iniciación, planificación, ejecución, monitoreo y control y cierre. Las nueve áreas de conocimiento que indica el PMBOK son las gestiones de: integración, alcance, tiempo, costos, calidad, RRHH, riesgos y adquisiciones del proyecto.

Para el diseño de este proyecto se limitará a tomar en cuenta exclusivamente cuatro de las nueve áreas de conocimiento que abarca el PMBOK. Las áreas que se tomarán en cuenta son las gestiones de alcance, tiempo, calidad y riesgos del proyecto. Asimismo, como solo es un proyecto de diseño, el proyecto se limitará a cubrir con los procesos de iniciación y planificación en la mayoría de aspectos dentro del mismo, mas no los procesos de ejecución, monitoreo y control y cierre. Esto es debido a que no se implementará el SGSI diseñado dentro del instituto educativo.

## 8. Justificación y viabilidad

El SGSI que se diseñará en el presente proyecto protegerá al instituto educativo frente a amenazas y riesgos que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de negocio. Enfocándose, principalmente, en proteger y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información que dan soporte a los procesos de negocio establecidos como alcance.

En conjunto con lo mencionado, dicha institución obtendrá algunas otras ventajas importantes con el diseño del SGSI para el presente proyecto de fin de carrera:



- Debido a la adaptación y establecimiento de un conjunto de controles establecidos internacionalmente por la norma ISO/IEC 27002, se logrará reducir las amenazas que puedan afectar los procesos “core” del instituto educativo y, en caso se logre materializar, que los daños que pueda ocasionar sean mínimos, de tal manera que la continuidad del negocio y la reputación del instituto estén aseguradas.
- La seguridad de información dejará de ser una actividad poco organizada y poco apoyada por los miembros del instituto educativo, para ser un conjunto de actividades metódicas y controladas, logrando instalarse en la cultura organizacional, siendo todos los empleados del instituto sus protagonistas y responsables. Entre otras cosas, incrementará la conciencia en seguridad entre los empleados, alumnos, representantes legales, etc.
- Finalmente, si en el futuro se evalúa la posibilidad de ejecutar la implementación -en conjunto de su respectiva certificación- del SGSI diseñado en la presente tesis, la institución educativa obtendría una ventaja competitiva frente a sus competidores, diferenciándola del resto de instituciones educativas e incrementando su prestigio e imagen frente a posibles clientes.

## 9. Plan de proyecto

### 9.1. Estructura de Descomposición del Trabajo (WBS)

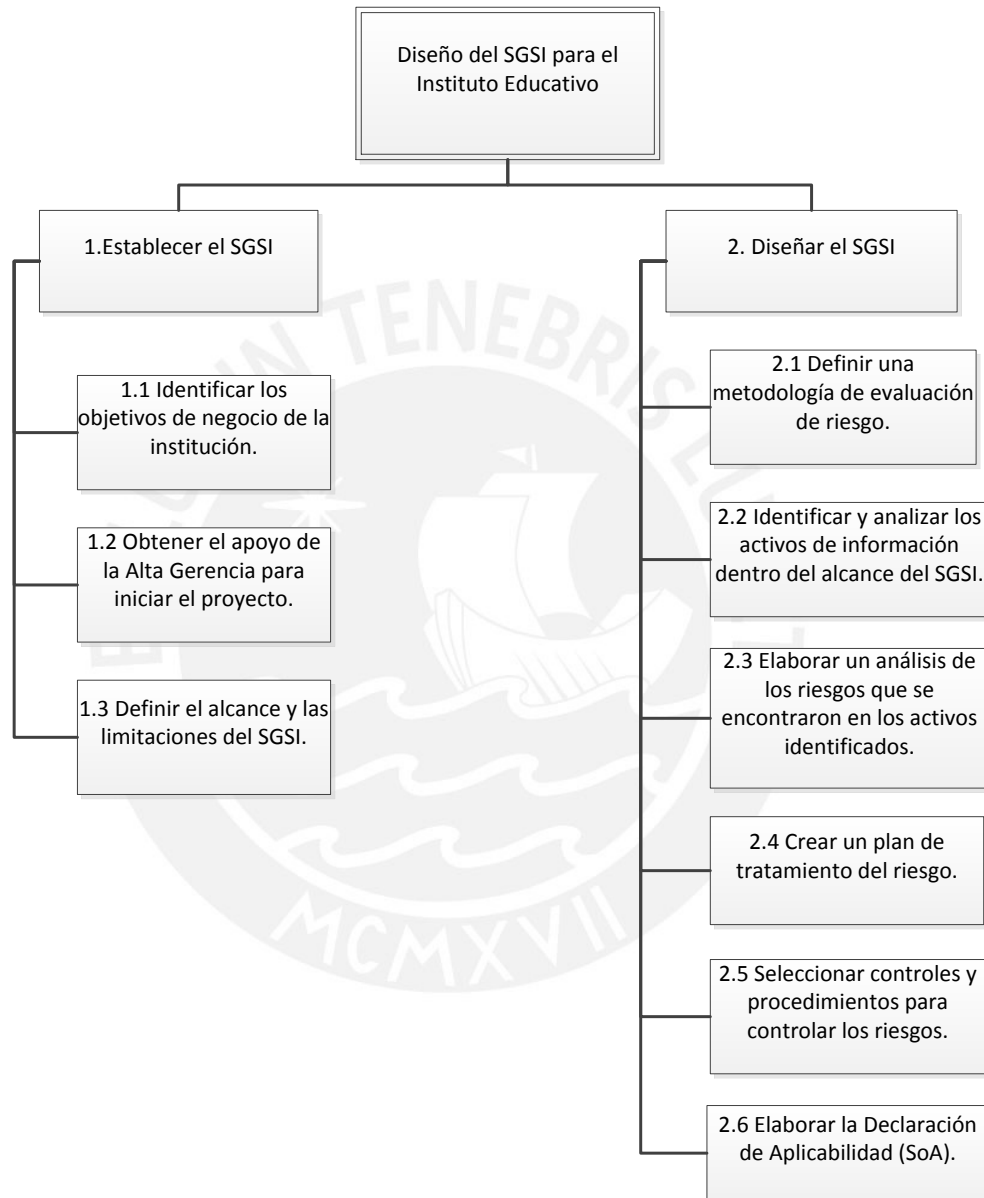


Figura 2. EDT del proyecto.

## 9.2. Diagrama de Gantt

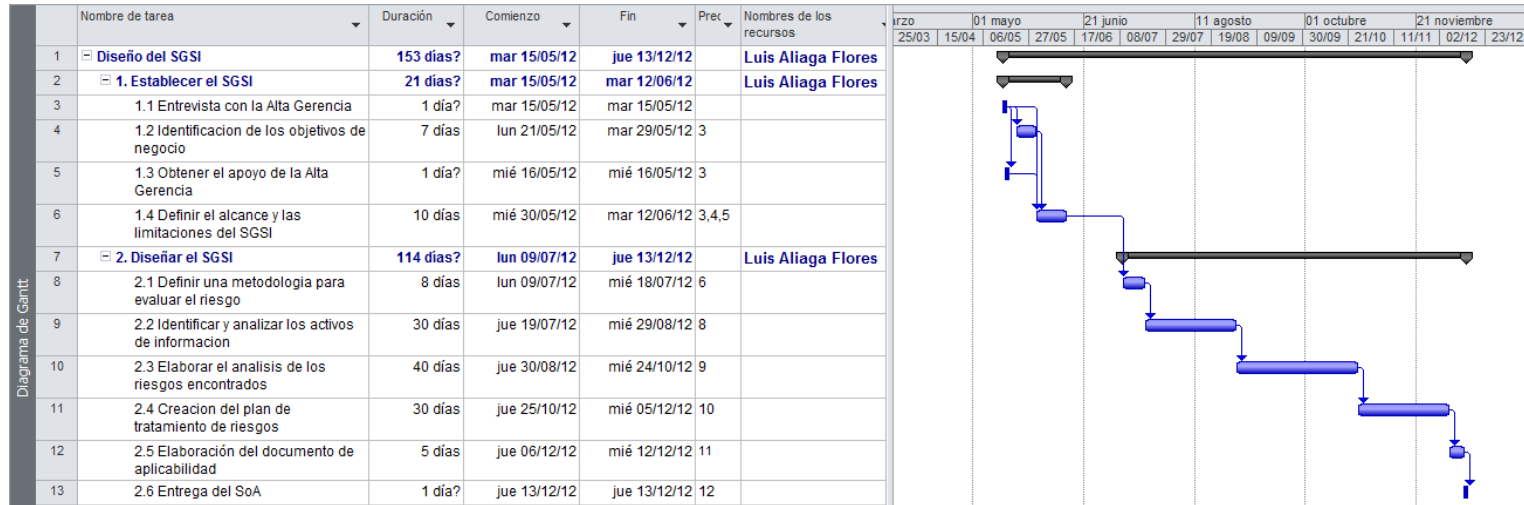


Figura 3. Diagrama de Gantt del proyecto.

## 10. Marco conceptual

En ese capítulo se estudiará y desarrollará el marco conceptual que se tiene que tomar en cuenta para poder comprender, de manera adecuada, lo que abarca un SGSI. Este marco contendrá un conjunto de términos y definiciones que se usarán a menudo en el presente proyecto. Asimismo, los institutos educativos a nivel superior que deseen implementar un SGSI bajo estándares internacionales deberán seguirán los procesos y procedimientos establecidos por la normas ISO/IEC 27001:2005, usando los controles establecidos en ISO/IEC 27002:2005, siguiendo la guía de propuesta por la ISO/IEC 27003:2010 y aplicando la metodología de tratamiento de riesgos propuesta por la ISO/IEC 27005:2008, usando el nuevo marco de trabajo COBIT 5 como contenedor de dichas normas. Estos estándares y buenas prácticas internacionales citados son las que se han se han desarrollado hasta el momento conforme al diseño y la implementación de un SGSI en cualquier organización.

### 10.1. Conceptos clave

En esta sección se presentan los conceptos relacionados a un Sistema de Gestión de Seguridad de Información.

#### 10.1.1. Activo

Cualquier elemento o información, tenga o no valor contable para la organización. [3]

##### 10.1.1.1. Control

Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. [6]

#### **10.1.1.2. Información**

Es un activo esencial para el negocio de una organización. Puede existir de muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. [6]

#### **10.1.1.3. Confidencialidad**

La propiedad que información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. [3]

#### **10.1.1.4. Disponibilidad**

La propiedad tiene que estar disponible y utilizable cuando lo requiera una entidad autorizada. [3]

#### **10.1.1.5. Integridad**

La propiedad de guardar la exactitud e integridad de los activos. [3]

#### **10.1.2. Seguridad de Información**

Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. [6]

#### **10.1.2.1. Evento de seguridad de información**

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. [4]

#### **10.1.2.2. Incidente de seguridad de información**

Es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. [4]

#### **10.1.3. Sistema de gestión de seguridad de información (SGSI)**

Es parte del sistema de gestión general, basada en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información. [5]

##### **10.1.3.1. Proyecto de SGSI**

Actividades estructuradas llevadas a cabo por la organización con el fin de implementar un SGSI. [7]

#### **10.1.4. Amenaza**

Una causa potencial de un incidente no-deseado, el cual puede resultar dañando a un sistema. [3]

#### **10.1.5. Vulnerabilidad**

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. [3]

#### **10.1.6. Riesgo**

Es la combinación de la probabilidad de un evento y su ocurrencia [2]

#### **10.1.6.1. Análisis de riesgo**

Uso sistemático de la información para identificar fuentes y para estimar el riesgo. Identifica los activos a proteger o evaluar. [6]

#### **10.1.6.2. Evaluación del riesgo**

Proceso de comparar el nivel de riesgo estimado durante el proceso de análisis de riesgo con un criterio dado para determinar la importancia del riesgo. [2]

#### **10.1.6.3. Gestión del riesgo**

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. Normalmente incluye la evaluación, tratamiento, aceptación y comunicación del riesgo. Estas actividades se enfocan a manejar la incertidumbre relativa de las amenazas detectadas. [2]

#### **10.1.6.4. Tratamiento del riesgo**

Proceso de tratamiento de la selección e implementación de controles para modificar el riesgo. [2]

#### **10.1.6.5. Riesgo residual**

El riesgo remanente después del tratamiento del riesgo. [2]

#### **10.1.6.6. Aceptación del riesgo**

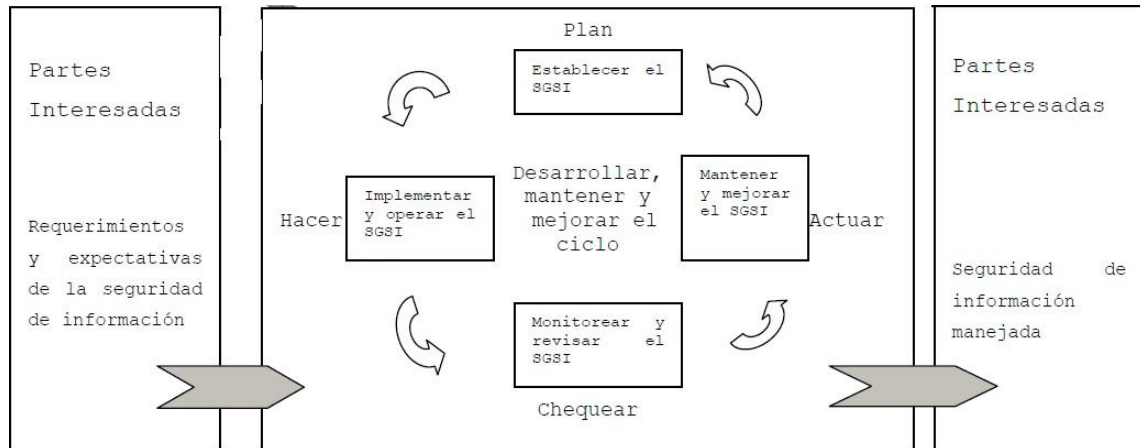
Decisión de aceptar el riesgo. [2]

#### **10.1.7. Política**

Intención y dirección general expresada formalmente por la gerencia. [6]

### **10.2. ISO/IEC 27001:2005**

Este estándar internacional “proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información dentro de cualquier organización”[5]. Indica las acciones que tiene que realizar una organización para poder alinearse a los requerimientos que tiene un SGSI. Para todos los procesos dentro del SGSI, la norma se basa en el modelo Plan-Do-Check-Act, el cual toma como input las expectativas que las partes interesadas de la organización tienen con respecto a la seguridad de información y, siguiendo este plan PDCA, produce un output de seguridad de información que satisfacen aquellas expectativas.



**Figura 4. Modelo PDCA aplicado a los procesos de un SGSI. [5]**

### 10.3. ISO/IEC 27002:2005

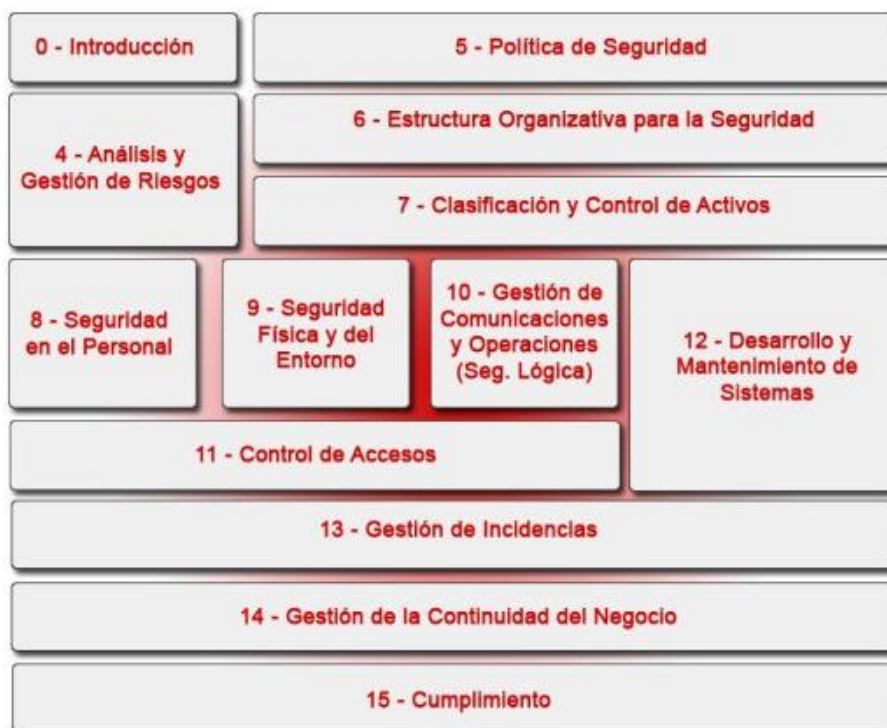
Este estándar internacional “establece los lineamiento y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de información en una organización” [6]. Nos da marcos de control necesarios para la implementación de un SGSI. Contiene once cláusulas de control de seguridad y cada una de estas cláusulas contiene un número de categorías de seguridad principales. A su vez, cada una de estas categorías de seguridad tiene un objetivo de control que es lo que se quiere lograr y los controles que se pueden aplicar para lograr dicho objetivo.

Las once clausulas mencionadas previamente son:

- Política de Seguridad
- Organización de la Seguridad de Información
- Gestión de Activos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones



- Control de acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de Seguridad de Información
- Gestión de la Continuidad Comercial
- Conformidad



**Figura 5. Secciones del ISO 27002 [6]**

Este estándar tiene una clausula introductoria que nos habla sobre la evaluación y el tratamiento de los riesgos de seguridad: identificar, priorizar y cuantificar los riesgos que la organización está expuesta, determinando cuales pueden ser riesgos aceptables y cuales riesgos son relevantes para la organización. Estos últimos se tienen que tratar según ciertos controles apropiados indicados en este estándar u otro conjunto de controles.

#### **10.4. ISO/IEC 27003:2010**

Este estándar internacional es nuestra guía para la implementación de un SGSI dentro de la institución educativa. Este documento explica dicha implementación enfocándose en la iniciación, planeamiento y la definición del proyecto: describe los

procesos desde la obtención de la aprobación de la alta gerencia para implementar el SGSI hasta la conclusión final del plan de proyecto

A diferencia del ISO 27001, este documento nos da recomendaciones y buenas prácticas, mas no indica requerimientos ni obligaciones: es para el uso en conjunto con la norma ISO 27001 y no para modificar o reducir los requerimientos especificados en dicha norma.

El proceso del planeamiento de la implementación de un SGSI contienen cinco fases y cada fase es representada por una clausula. Todas estas cláusulas tienen una estructura similar: cada clausula tiene uno o varios objetivos y una o varias actividades necesarias para lograr dichos objetivos.

Las cinco fases son:

- Obtención de la aprobación de la alta gerencia para iniciar el proyecto de SGSI.
- Definición del alcance las políticas del SGSI.
- Conducir el análisis de la organización.
- Conducir un análisis de riesgos y un plan de tratamiento de riesgos.
- Diseñar el SGSI.

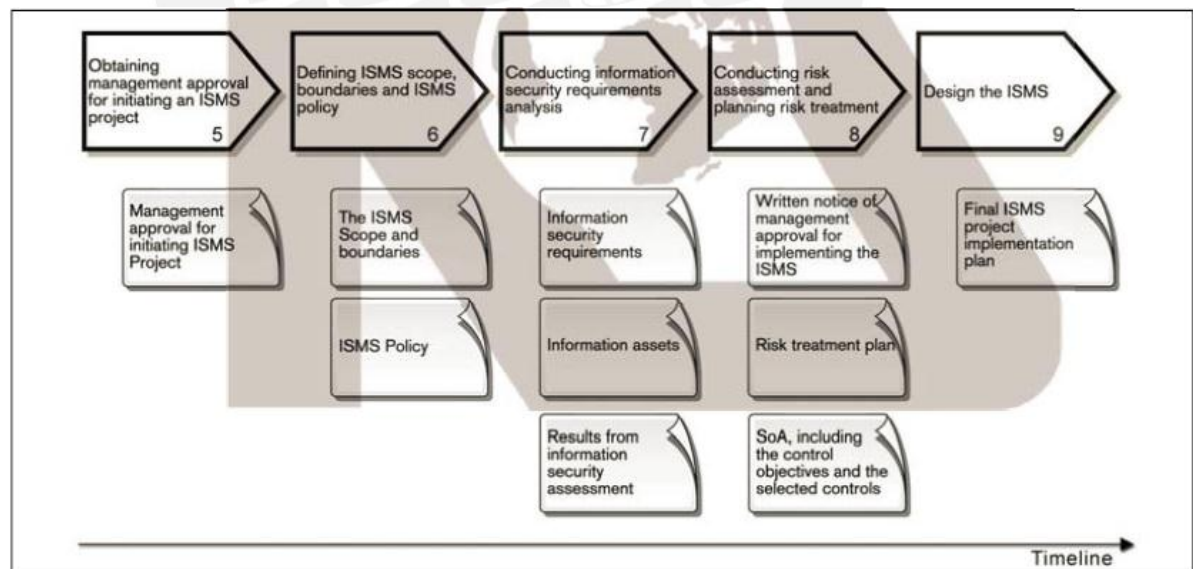


Figura 6. Fases de un proyecto de SGSI [7]

## 10.5. ISO/IEC 27005:2008

Este estándar internacional nos brinda directrices para la gestión de riesgos de la seguridad de información, dando soporte particularmente a los requerimientos de un SGSI, de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no es de por sí una metodología para la gestión de riesgos, aunque lo puede llegar a ser según el alcance que el SGSI tenga o el contexto de la gestión de riesgos donde se aplique dicha norma.

La estructura de la norma se descompone en 12 cláusulas, las cuales son:

- Clausula 1: Alcance.
- Clausula 2: Referencias normativas.
- Clausula 3: Términos y definiciones.
- Clausula 4: Estructura de la norma.
- Clausula 5: Background.
- Clausula 6: Resumen del proceso de la gestión de los riesgos de la seguridad de información.
- Clausula 7: Establecimiento del contexto.
- Clausula 8: Risk Assessment.
- Clausula 9: Risk Treatment.
- Clausula 10: Risk Acceptance.
- Clausula 11: Risk Communication
- Clausula 12: Risk Monitoring.

La siguiente figura ilustra que el proceso de la gestión de los riesgos de la seguridad de información puede ser iterativo para la evaluación de los riesgos y/o las actividades que envuelvan el tratamiento de los mismos. Este enfoque iterativo que propone la norma nos puede incrementar la profundidad y el detalle en la evaluación de los riesgos en cada iteración, así como un balance adecuado entre minimizar el tiempo y el esfuerzo en identificar controles adecuados y asegurar que los riesgos con alto impacto y/o posibilidad de ocurrencia estén debidamente monitoreados.

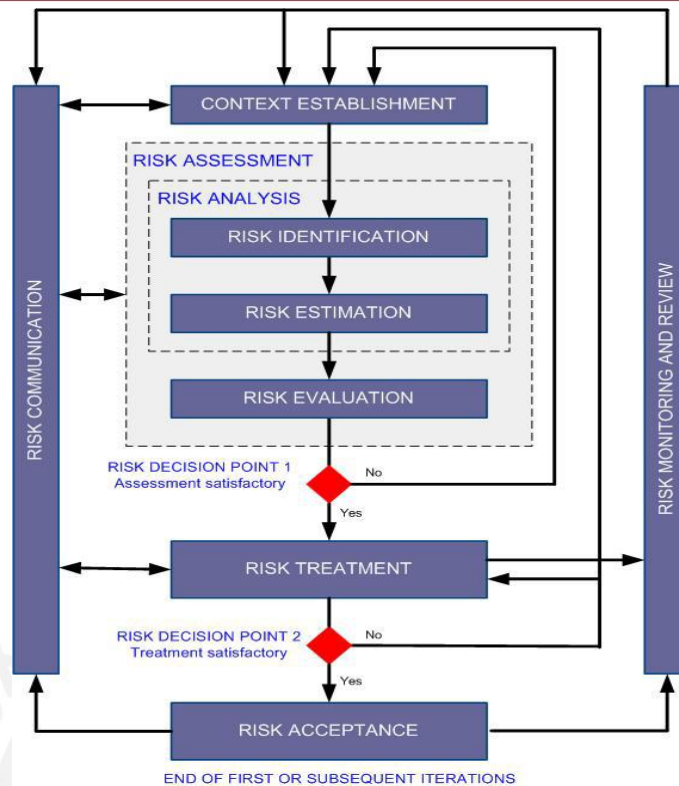


Figura 7. Proceso de la gestión de riesgos de seguridad de información [12]

## 10.6. COBIT 5

COBIT 5 provee un marco de referencia para asistir a las empresas y organizaciones a que alcancen sus objetivos de negocio y entregar valor a través de un gobierno eficiente y una buena gestión de sus tecnologías de información. Con esto las empresas se aseguran de que están entregando valor y obteniendo confianza de la información y sus sistemas, afrontando los retos a los que se enfrentan en la actualidad.

COBIT 5 tiene una perspectiva de negocio, no solo de TI. Este es el principal cambio frente a sus anteriores ediciones. Este framework puede ser usado por cualquier usuario de cualquier área de la empresa. Asimismo, puede ser tomado como referencia por cualquier stakeholder que tenga la organización.

COBIT 5 está basado en cinco principios clave:

- **Principio 1: Satisfacer las necesidades de los Stakeholders**

Las empresas existen para crear valor a sus Stakeholders. Esto se logra manteniendo un balance entre los objetivos de negocio, la optimización

de los riesgos que puedan existir y el uso de recursos dentro de la organización. COBIT 5 provee todos los procesos requeridos y otros habilitadores para dar soporte a la creación de valor a través del uso de las tecnologías de información.

- **Principio 2: Cubrir la organización de principio a fin:**  
COBIT 5 cubre todas las funciones y procesos dentro de la empresa. No solo se enfoca en la parte de TI, sino que trata a la información y a la tecnología como activos que necesitan ser tratados como otro cualquier activo dentro de la empresa.
- **Principio 3: Aplicar un único marco de trabajo integrado**  
Hay varios estándares relacionados a las tecnologías de información y sus buenas prácticas. COBIT 5 se alinea con estos estándares y frameworks en un alto nivel y puede ser utilizado como un marco contenedor de todos estos.
- **Principio 4: Aproximación holística**  
COBIT 5 define un conjunto de habilitadores para dar soporte a la implementación de un gobierno y una gestión comprensiva de TI. Estos habilitadores son definidos como cualquier cosa que pueda ayudar a alcanzar los objetivos de negocio de la organización. Más adelante se definirán los siete habilitadores que propone COBIT 5.
- **Principio 5: Separar “Gestión” de “Gobierno”**  
COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas tienen diferentes tipos de actividades, requieren distintas estructuras organizacionales y sirven para diferentes propósitos

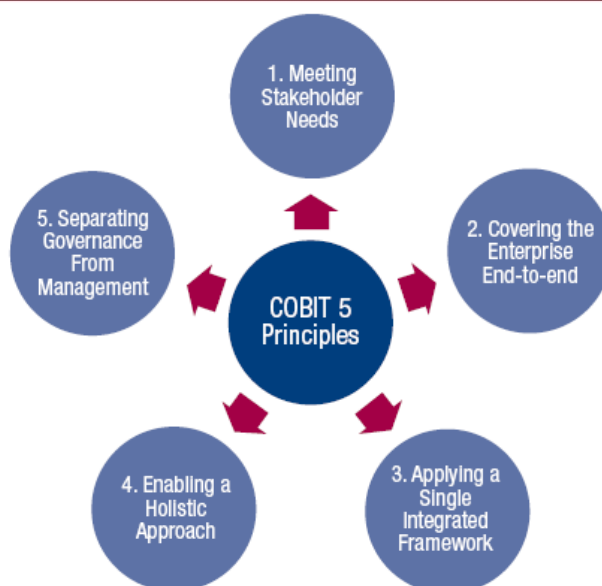
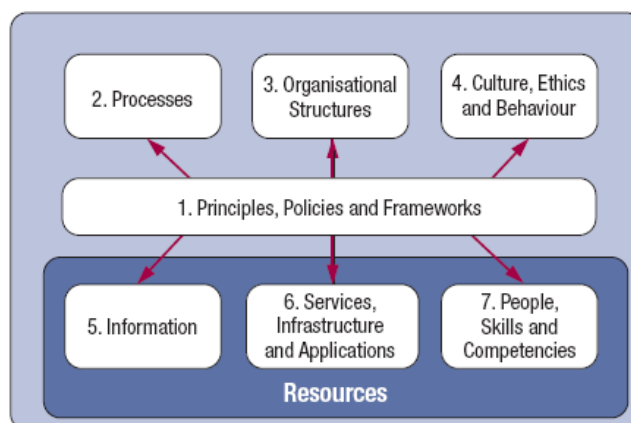


Figura 8. Los 5 principios del marco COBIT 5 [8]

Asimismo, COBIT 5 nos define siete categorías de habilitadores:

1. **Principios, políticas y marcos de trabajo** son el medio para trasladar el comportamiento deseado a una guía práctica para la conducir la gestión del día-a-día.
2. **Procesos** constituyen un conjunto organizado de prácticas y actividades para producir los outputs respectivos para alcanzar las metas de TI
3. **Estructura organizacional** son las entidades que toman las decisiones críticas en la organización
4. **Cultura, ética y comportamiento** de los individuos y de la empresa son muy frecuentemente sobrestimados como un factor de éxito de los objetivos de gobierno y gestión establecidos.
5. **La Información** está en todos los ámbitos de la organización. Es requerida para mantener a la organización andando y bien gestionada. Asimismo, en un nivel operacional, la información es pieza clave.
6. **Servicios, infraestructura y aplicaciones** dan soporte a los procesos y servicios de TI
7. **Personas, habilidades y competencias** están conectadas a las personas. Son requeridas para tomar decisiones correctas y tomar acciones correctivas adecuadas.

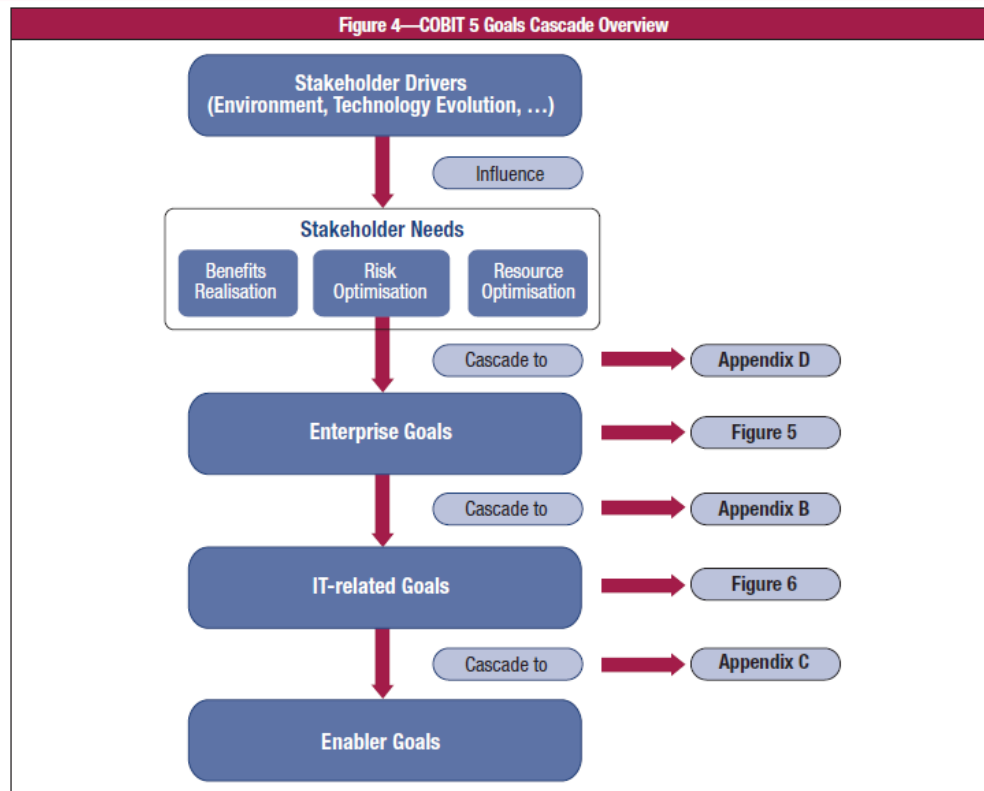




**Figura 9. Los siete principios del marco COBIT 5 [8]**

Finalmente, COBIT 5 nos introduce una cascada de objetivos la cual permite definir las prioridades para la implementación, mejora y aseguramiento del gobierno de TI basada en los objetivos de negocio de la organización y el posible riesgo al que este expuesta. Principalmente, la cascada de objetivos:

- Define los objetivos más relevantes y tangibles en varios niveles de responsabilidad.
- Permite extraer la información más relevante del conocimiento base de COBIT 5 para su inclusión en proyectos específicos.
- Identifica y comunica claramente como los habilitadores son importantes para alcanzar los objetivos organizacionales.



**Figura 10. La cascada de objetivos de COBIT 5 [8]**

## 11. Revisión del estado del arte

En la actualidad ninguna institución educativa ni universidad está certificada en la norma ISO 27001 dentro del contexto educativo peruano según una investigación del mercado educativo que se realizó para la presente tesis. Sin embargo, en este punto se mencionarán las universidades e instituciones educativas internacionales más importantes que sí han obtenido la certificación ISO/IEC 27001 hasta la fecha.

### 11.1. Universidad Nacional de Ciencia y Tecnología de Taiwán

La Universidad Nacional de Ciencia y Tecnología de Taiwán, NTUST por sus siglas en inglés, se creó el primero de Agosto en 1974 como el primer instituto educativo del tipo tecnológico dentro de Taiwán. Actualmente cuentan con 4953 alumnos, 48337 graduados y 336 profesores a tiempo completo.

Al alcanzar el estado de “Universidad” en 1997, la escuela se reorganizó en 5 facultades: ingeniería, ingeniería eléctrica y de sistemas, gestión, diseño y arte y



ciencias sociales. Entre los departamentos se incluyen los programas de ingeniería mecánica, ingeniería civil, ingeniería química, ingeniería informática, etc. En conjunto con las carreras de ingeniería, el departamento de humanidades ofrece programas de humanidades y ciencias sociales, así como el departamento de educación ofrece programas a para futuros profesores. Todos los departamentos juntos forman 21 programas que la Universidad Nacional de Ciencia y Tecnología de Taiwán ofrece. Finalmente aceptan estudiantes para programas de pregrado, maestrías y doctorado.

En Abril del 2011, el SGS (Société Générale de Surveillance) en Taiwán, una compañía certificadora reconocida a nivel mundial, le entrego la certificación de la ISO 27001 a la universidad NTUST, mencionando que la calidad de la gestión de la seguridad de información de la NTUST alcanza los más altos estándares de calidad e integridad hoy en día a nivel mundial.

La certificación mencionada cubre los procesos de mantenimiento y operación del centro de cómputo de NTUST y el desarrollo, operación y mantenimiento de todos los sistemas de información de los alumnos. Las compañías de certificación visitaban el campus de vez en cuando para una serie de inspecciones de documentación e in-situ. Asimismo, condujeron una serie de entrevistas con los administradores de los sistemas para verificar si cada módulo de los sistemas de información está asegurado adecuadamente. Finalmente, luego de 10 meses de las fases de planeamiento e implementación que el estándar ISO 27001 demanda que se realice, en conjunto con las inspecciones de la entidad certificadora, la NTUST logro dicha certificación.

## **11.2. Universidad Libre de Bozen/Bolzano**

La Universidad Libre de Bozen/Bolzano es fundada el 31 de Octubre de 1997 en Italia como una institución educativa orientada a la internalización y pluralidad de lenguas. Dicha universidad, promueve el libre intercambio de ideas y conocimiento científico, vinculándose con la tradición europea de humanidades y el respeto por los principios democráticos.

Actualmente cuenta con 5 facultades: la facultad de ciencias de la computación, la escuela de administración y economía, la facultad de educación, la facultad de diseño y de arte y finalmente, la facultad de ciencias y tecnología. Cabe resaltar que tiene 3 campus y enseñan en 4 distintos lenguajes: inglés, alemán, italiano y latín. Finalmente, cuentan con 3364 estudiantes actualmente, los cuales el 18% son de origen internacional, lo que demuestra que alientan el intercambio cultural estudiantil.

El 12 de Enero del 2007 la Universidad Libre de Bozen/Bolzano recibió la certificación ISO 27001. Esta universidad es la primera organización científica a nivel mundial en obtener en la certificación en el ISO 27001.

Por una semana, dicha universidad estuvo auditada por dos entidades certificadoras: ÖQS (Austrian Association for certification of quality and management systems) y CIS (Certification & Information Security Services). Ellas estuvieron auditando y verificando que todo el proceso de transferencia del conocimiento de la información (desde la infraestructura de bases de datos hasta el código de conducta dentro de la universidad) en la institución estuviera lo suficientemente segura, como lo exige la norma que se maneja.

En conjunto con dicha certificación, el departamento de informática y comunicaciones, encargada de gestionar la red informática de la universidad y el desarrollo del software interno educativo, obtuvo también la certificación ISO 9001:2000 por la calidad de sus sistemas de gestión, siendo el primer y único departamento en la Universidad Libre de Bozen/Bolzano que maneja dichas certificaciones.

### 11.3. Universidad Kyushu

La universidad Kyushu es una universidad ubicada en Japón la cual se fundó en 1903 con solo dos carreras universitarias: medicina e ingeniería. Desde ese entonces, varias reformas se han hecho para alcanzar un mejor sistema educacional en Japón como la introducción de nuevos formatos educativos después de la segunda guerra mundial y la reorganización de las universidades de Japón en el 2004.

El total de estudiantes de esta universidad es de 18765 aproximadamente, mientras que los miembros de la facultad son de 2186. Asimismo, los programas de intercambio son alentados ya que aceptan a varios estudiantes de intercambio cada año. En la actualidad hay más de 1700 estudiantes de aproximadamente 8 países estudiando dentro de la universidad Kyushu.

El 3 de Abril del presente año, esta universidad recibió la certificación ISO/IEC27001 a través del vicepresidente de TI Hiroto Yusuura por parte del BSI (British Standards Institution).

## 12. Discusión sobre los resultados de la revisión del estado del arte

De todo lo estudiado y analizado previamente podemos observar que, si bien existen algunas instituciones educativas internacionales certificadas en el ISO 27001, estas no abundan en el panorama mundial. En el contexto peruano, según no existe ni una sola institución o universidad educativa certificada en dicho estándar, lo cual demuestra que aún no se le da la importancia adecuada a la información frente a la problemática actual descrita previamente y los diversos panoramas negativos que la falta de dichos controles puedan traer.

Asimismo, si bien es cierto que se cuenta con una gran cantidad de información con respecto a las buenas prácticas en la seguridad de información, el panorama organizacional que se asume en la literatura estudiada siempre supone a una empresa ordenada y puntual con respecto a los procesos que se lleven a cabo y la documentación que la misma tiene. Lamentablemente, en el caso peruano, no es común que dicho modelo de empresa abunde en nuestra sociedad. Por lo general, nos vamos a encontrar con empresas informales en diversos aspectos, algunas inclusive teniendo muy poca noción sobre sus propios procesos principales, ni mucho menos sobre la documentación que manejen o que generen dichos procesos.

## Capítulo 2: Procesos de un instituto educativo

### 1. Modelamiento de los procesos “core” de un instituto educativo

Como se mencionó en el punto 6.1 del capítulo 1, el alcance que tendrá el presente proyecto involucra a los principales procesos del instituto educativo estudiado, conocidos como procesos “core”. Estos procesos se modelarán siguiendo la notación BPMN 2.0 (Business Process Modeling Notation) la cual es una notación gráfica estandarizada que permite observar de manera detallada todo el flujo de trabajo que siguen dichos procesos.

A continuación se procederá a describir y detallar estos procesos “core” de una entidad educativa local de nivel superior.

#### 1.1. Proceso de Diseño y Desarrollo de Nuevos Productos

##### A. *Objetivo*

Asegurar que el diseño y desarrollo de las nuevas carreras y cursos respondan a las necesidades de la sociedad, del público objetivo y de la misión de la institución educativa, considerando también la normatividad vigente.

### *B. Responsable del proceso*

Director Académico (a nivel corporativo).

### *C. Definiciones*

- Diseño curricular: define la estrategia que cuenta con una serie de pasos organizados y estructurados con el fin de elaborar un currículo. Propone la definición de una estrategia para la instrumentación del sistema de gestión del proceso curricular como aporte práctico y de esta forma pueda ser introducida en los procesos académicos y académico-administrativos con la finalidad de lograr un mejoramiento permanente de la enseñanza y aprendizaje: la articulación de cursos, jerarquización de logros y contenidos, material didáctico, la evaluación, eficacia del proceso enseñanza –aprendizaje, entre otras actividades.
- Currículo: es el diseño estructurado de experiencias de aprendizaje que en forma intencional son articuladas con la finalidad de producir los aprendizajes esperados en los estudiantes. Conjunto de competencias básicas, objetivos, contenidos, criterios metodológicos y de evaluación que los estudiantes deben alcanzar en un determinado nivel educativo.

### *D. Diagrama del proceso*

Ver Anexo 1.1

## **1.2. Procesos de Programación Académica y de Recursos**

Este proceso se compone de tres subprocesos, los cuales abarcan desde la programación de la frecuencia de los programas o carreras que tendrán durante el año, hasta la programación de los recursos principales, como son los profesores (o facilitadores como se le dice en la entidad educativa tomada como referencia) y las aulas dentro de la sede correspondiente.

### **1.2.1. Proceso de Programación de Frecuencias**

#### *A. Objetivo*

Generar y registrar en el sistema la programación de frecuencias (inicios de semestres) de manera oportuna para facilitar la planificación de las actividades académicas, comerciales y de soporte necesarias para una adecuada prestación del servicio educativo.

*B. Responsable del proceso*

Gerente de Sede.

*C. Definiciones*

No aplica.

*D. Diagrama del proceso*

Ver Anexo 1.2

### **1.2.2. Proceso de Programación de Facilitadores**

*A. Objetivo*

Designar a los facilitadores para el dictado de una asignatura, considerando el cumplimiento de perfiles docentes y los niveles de exigencia requeridos para cada programa académico.

*B. Responsable del proceso*

- Director Académico: Define los lineamientos procesos para la programación de facilitadores.
- Gerente de Sede (en cada sede): Ejecuta y toma las decisiones finales para la programación de sus facilitadores.

*C. Definiciones*

- Evaluación de 360°: es una herramienta integral de evaluación en el que el facilitador es calificado por su entorno académico para proporcionarle información relevante y objetiva sobre su desempeño, ayudándolo a identificar sus fortalezas y los aspectos que debe mejorar. Entre los elementos que se consideran en la evaluación se tienen: las encuestas académicas, la autoevaluación del facilitador, la evaluación de Secretaría Académica, la evaluación del Jefe Académico y los resultados del monitoreo al facilitador.
- Evaluación del Jefe Académico: es la valoración que realiza el Jefe Académico sobre el facilitador con respecto al cumplimiento de sus funciones. Entre los aspectos a evaluar se tienen: el uso de materiales de estudio, asistencia a las reuniones de coordinación y de trabajo en equipo.

*D. Diagrama del proceso*

Ver Anexo 1.3

### 1.2.3. Proceso de Programación de Aulas

#### A. *Objetivo*

Ordenar y agilizar el proceso de programación de aulas con la finalidad de brindar un mejor servicio y mayor comodidad a los alumnos durante el proceso de ejecución.

#### B. *Responsable del proceso*

Jefe de Servicios Educativos

#### C. *Definiciones*

Semestre secuencial: es un periodo de estudios de la carrera a partir del segundo semestre.

#### D. *Diagrama del proceso*

Ver Anexo 1.4

## 1.3. Procesos de Captación y Admisión de Alumnos

Este proceso se compone de dos subprocesos, los cuales abarcan desde la organización de las charlas informativas de los programas y carreras que la institución educativa ofrece para la captación de potenciales clientes, hasta la venta de estas carreras y programas a los clientes interesados.

### 1.3.1. Proceso de Organización de Charlas Informativas

#### A. *Objetivo*

Optimizar el proceso de convocatoria a charlas informativas de manera que se pueda obtener la mayor cantidad de participantes así como también proporcionar la información pertinente al área de Ventas acerca de los potenciales clientes a captarse en dichas charlas y de esta manera facilitar el cumplimiento del logro de metas de captación

#### B. *Responsable del proceso*

Área de Telemarketing y Área de Ventas.

#### C. *Definiciones*

No aplica.

#### D. *Diagrama del proceso*

Ver Anexo 1.5



### 1.3.2. Proceso de Ventas de Carreras

#### A. *Objetivo*

Facilitar la captación de clientes y la venta de las carreras del Instituto Educativo

#### B. *Responsable*

Jefe Comercial o Supervisor de Ventas (dependiendo de la Sede)

#### C. *Definiciones*

- Cliente nuevo: se refiere a las personas interesadas en llevar uno de los programas académicos de la Institución por primera vez. Las matrículas de clientes nuevos son las que generan comisiones para los vendedores.
- Formulario de preinscripción: documento para el registro de datos del interesado, que servirá para el seguimiento a su inscripción en uno de los programas de la Institución. Este formulario es entregado en forma impresa, vía correo electrónico o fax, para que luego de completar la información necesaria, el interesado lo devuelva o reenvíe el área de ventas.
- Ingresante: se refiere a la persona que ha aprobado el proceso de admisión (evaluación de aptitud emprendedora).
- Postulante: se refiere a la persona interesada en llevar una de las carreras de la Institución y que para ello se ha inscrito en el proceso de admisión correspondiente.
- Reglamento de admisión: disposiciones académico-administrativas institucionales y legales para el desarrollo del proceso de admisión.

#### D. *Diagrama del proceso*

Ver Anexo 1.6

## 1.4. Procesos de Matrícula

Este proceso se compone de dos subprocesos de matrícula. El primero abarca la admisión y matrícula cuando es un cliente nuevo y aun no se tiene la condición de alumno, y el segundo abarca la matrícula de los alumnos regulares de la institución.



#### 1.4.1. Proceso de Admisión y Matricula de Ingresantes

##### A. *Objetivo*

Asegurar que los ingresantes a las carreras cumplan con los requisitos administrativos y el perfil de ingreso establecido.

##### B. *Responsable del proceso*

Jefe de Secretaría Académica

##### C. *Definiciones*

- Alumno: es la persona matriculada en cualquier de los programas académicos de la Institución.
- Ingresante: se refiere a la persona que ha aprobado el proceso de admisión (evaluación de aptitud emprendedora).
- Postulante: se refiere a la persona interesada en llevar una de las carreras de la Institución y que para ello se ha inscrito en el proceso de admisión correspondiente.
- Reglamento de admisión: disposiciones académico-administrativas institucionales y legales para el desarrollo del proceso de admisión.

##### D. *Diagrama del proceso*

Ver Anexo 1.7

#### 1.4.2. Proceso de Matricula Secuencial

##### A. *Objetivo*

Asegurar que el proceso de matrícula en semestres secuenciales se realice de manera efectiva y conciliar la información académica de las matrículas en los semestres secuenciales de las carreras de la Escuela de Empresarios.

##### B. *Responsable del proceso*

Jefe de Servicios Educativos

##### C. *Definiciones*

Cliente nuevo: registro o inscripción de los alumnos que van a realizar sus estudios en la institución educativa.

##### D. *Diagrama del proceso*

Ver Anexo 1.8

### 1.5. Proceso de Titulación

*A. Objetivo*

Asegurar que los alumnos obtengan el título a nombre de la nación que acredite la culminación satisfactoria de sus estudios.

*B. Responsable del proceso*

Jefe de Servicios Educativos.

*C. Definiciones*

No aplica.

*D. Diagrama del proceso*

Ver Anexo 1.9



## 2. Identificación de activos

En este punto se identificarán los activos que están envueltos en cada proceso descrito anteriormente. Según el estándar ISO 27005:2008, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según este estándar, son los procesos e información más sensibles para la organización. Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios. Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos:

- 1) **Dato:** Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la institución educativa gestiona dentro de sus procesos.
- 2) **Aplicación:** Todo aquel software que se utilice como soporte en los procesos.
- 3) **Personal:** Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización.
- 4) **Servicio:** Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.
- 5) **Tecnología:** Es todo el hardware donde se maneja la información y las comunicaciones.
- 6) **Instalación:** Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.
- 7) **Equipamiento auxiliar:** Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

A continuación, se muestra el inventario de todos los activos que se pudieron identificar dentro de los procesos del instituto educativo que se encuentran en el alcance del presente proyecto.

| ID | Activo identificado                              | ¿Tangible? | Tipo de Activo |
|----|--|------------|----------------|
| 1  | Computadora de escritorio                        | Si         | Tecnología     |
| 2  | Licencia de Microsoft Windows XP                 | No         | Aplicación     |
| 3  | Licencia de Microsoft Office 2007                | No         | Aplicación     |
| 4  | Página web del Instituto Educativo               | No         | Aplicación     |
| 5  | Intranet de la institución                       | No         | Aplicación     |
| 6  | Email (para el envío electrónico de información) | No         | Aplicación     |
| 7  | Teléfono   | Si         | Tecnología     |

| ID | Activo identificado                           | ¿Tangible? | Tipo de Activo        |
|----|---|------------|-----------------------|
| 8  | Impresora                                     | Si         | Tecnología            |
| 9  | Fotocopiadora                                 | Si         | Tecnología            |
| 10 | Scanner                                       | Si         | Tecnología            |
| 11 | Cableado Ethernet                             | Si         | Tecnología            |
| 12 | Red del instituto (carpetas compartidas)      | No         | Aplicación            |
| 13 | Firewall                                      | No         | Tecnología            |
| 14 | Aula  | Si         | Instalación           |
| 15 | Vitrinas informativas                         | Si         | Instalación           |
| 16 | Oficina de reuniones                          | Si         | Instalación           |
| 17 | Sistema de información SMART                  | No         | Aplicación            |
| 18 | Servidor para el sistema de información SMART | Si         | Tecnología            |
| 19 | Archivadores para los documentos              | Si         | Equipamiento Auxiliar |
| 20 | Archivos de la sede                           | Si         | Instalación           |
| 21 | Gabinetes                                     | Si         | Equipamiento Auxiliar |
| 22 | Llaves de ingreso                             | Si         | Equipamiento Auxiliar |
| 23 | Director Académico                            | Si         | Personal              |
| 24 | Stakeholder interno                           | Si         | Personal              |
| 25 | Stakeholder externo                           | Si         | Personal              |
| 26 | Gerente de Sede                               | Si         | Personal              |
| 27 | Jefe de Secretaría Académica                  | Si         | Personal              |
| 28 | Analista de procesos                          | Si         | Personal              |
| 29 | Director de Operaciones                       | Si         | Personal              |
| 30 | Director Comercial                            | Si         | Personal              |
| 31 | Jefe Académico                                | Si         | Personal              |
| 32 | Asistente de Programación                     | Si         | Personal              |
| 33 | Facilitador                                   | Si         | Personal              |
| 34 | Jefe de Servicios Educativos                  | Si         | Personal              |
| 35 | Jefe Comercial                                | Si         | Personal              |
| 36 | Telemarketer / Promotor de Ventas             | Si         | Personal              |

| ID | Activo identificado  | ¿Tangible? | Tipo de Activo |
|----|--|------------|----------------|
| 37 | Cliente  | Si         | Personal       |
| 38 | Alumno   | Si         | Personal       |
| 39 | Cajero   | Si         | Personal       |
| 40 | Asistente Administrativo   | Si         | Personal       |
| 41 | Calígrafo  | Si         | Personal       |
| 42 | Egresado   | Si         | Personal       |
| 43 | Asistente de Admisión  | Si         | Personal       |
| 44 | Asistente Académico  | Si         | Personal       |
| 45 | Jefe de Coordinación   | Si         | Personal       |
| 46 | Servidor web   | Si         | Tecnología     |
| 47 | Documento del perfil profesional de la nueva carrera (misión, perfil del egresado, etc.) | Si         | Dato           |
| 48 | Documento del nuevo plan de estudios   | Si         | Dato           |
| 49 | Información estratégica del instituto  | Si         | Dato           |
| 50 | Documento de información del análisis del mercado  | Si         | Dato           |
| 51 | Acta formal de constitución  | Si         | Dato           |
| 52 | Documento de encuestas   | Si         | Dato           |
| 53 | Documentos estadísticos del mercado educativo  | Si         | Dato           |
| 54 | Informe con el resultado de la investigación   | Si         | Dato           |
| 55 | Acta del comité consultivo   | Si         | Dato           |
| 56 | Documento de la proyección anual de la oferta educativa (presupuesto)                    | Si         | Dato           |
| 57 | Documento de la programación académica anual y mensual                                   | Si         | Dato           |
| 58 | Reporte de alumnos aptos para matricularse   | Si         | Dato           |
| 59 | Información de alumnos de semestres anteriores   | Si         | Dato           |
| 60 | Impreso de la programación de frecuencias  | Si         | Dato           |
| 61 | Plan semestral/anual de cursos a dictarse  | Si         | Dato           |
| 62 | Evaluación 360°  | Si         | Dato           |
| 63 | Evaluación del Jefe Académico  | Si         | Dato           |
| 64 | Encuesta académica   | Si         | Dato           |
| 65 | Registro de información del facilitador  | Si         | Dato           |

| ID | Activo identificado   | ¿Tangible? | Tipo de Activo |
|----|---|------------|----------------|
| 66 | Documento de programación tentativa de facilitadores              | Si         | Dato           |
| 67 | Documento de programación de facilitadores                        | Si         | Dato           |
| 68 | Materiales de estudio (silabo, presentaciones, casos, lecturas)   | Si         | Dato           |
| 69 | Información sobre la evaluación de la "Evaluación 360°"           | Si         | Dato           |
| 70 | Resultado de calificaciones de la "Evaluación 360°"               | Si         | Dato           |
| 71 | Registro de aulas   | Si         | Dato           |
| 72 | Documento de frecuencia de cursos por campaña                     | Si         | Dato           |
| 73 | Documento de alumnos inscritos por campaña                        | Si         | Dato           |
| 74 | Documento de la programación de las aulas                         | Si         | Dato           |
| 75 | Base de datos de potenciales clientes                             | Si         | Dato           |
| 76 | Servidor para la base de datos de potenciales clientes            | Si         | Tecnología     |
| 77 | Informe de resultados de llamadas a clientes                      | Si         | Dato           |
| 78 | Información sobre preferencias de los clientes                    | Si         | Dato           |
| 79 | Guión de comunicación e información de productos                  | Si         | Dato           |
| 80 | Material informativo / Documentación relacionada a los programas  | Si         | Dato           |
| 81 | Brochure del programa   | Si         | Dato           |
| 82 | Reglamento de admisión  | Si         | Dato           |
| 83 | Formulario de Preinscripción                                      | Si         | Dato           |
| 84 | Ficha de Admisión   | Si         | Dato           |
| 85 | Registro de orden de cobro a los clientes inscritos               | Si         | Dato           |
| 86 | Consolidado de la información de las fichas de admisión (virtual) | Si         | Dato           |
| 87 | Evaluación de Aptitud Emprendedora (Examen de admisión)           | Si         | Dato           |
| 88 | Resultados de la Evaluación de Aptitud Emprendedora               | Si         | Dato           |
| 89 | Certificado original de estudios de 1° a 5° de secundaria         | Si         | Dato           |
| 90 | Partida de nacimiento original (o copia legalizada)               | Si         | Dato           |
| 91 | Fotocopia de DNI  | Si         | Dato           |
| 92 | Voucher de pago de Admisión                                       | Si         | Dato           |
| 93 | Ficha de Admisión (en físico)                                     | Si         | Dato           |
| 94 | Ficha de Matricula (en físico)                                    | Si         | Dato           |

| ID  | Activo identificado                           | ¿Tangible? | Tipo de Activo |
|-----|---|------------|----------------|
| 95  | Reporte de alumnos matriculados (en físico)   | Si         | Dato           |
| 96  | Ficha de preinscripción de matrícula          | Si         | Dato           |
| 97  | Consolidación bancaria (vía email)            | No         | Dato           |
| 98  | Voucher de pago de matrícula                  | Si         | Dato           |
| 99  | Registro de las matrículas                    | Si         | Dato           |
| 100 | Solicitud o cartas de descuento               | Si         | Dato           |
| 101 | Reporte visado de cartas de descuento         | Si         | Dato           |
| 102 | Solicitud de expedición del título            | Si         | Dato           |
| 103 | Ficha de inscripción para la titulación       | Si         | Dato           |
| 104 | Declaración jurada del egresado               | Si         | Dato           |
| 105 | Certificado de estudios superiores (original) | Si         | Dato           |
| 106 | Foto  | Si         | Dato           |
| 107 | Recibo de pago por derecho de titulación      | Si         | Dato           |
| 108 | Acta visada por la DRE                        | Si         | Dato           |
| 109 | Formato del Ministerio de Trabajo             | Si         | Dato           |
| 110 | Diploma                                       | Si         | Dato           |
| 111 | Acta de sustentación de tesis                 | Si         | Dato           |
| 112 | Título de egresado                            | Si         | Dato           |
| 113 | Fotocopia del título de egresado              | Si         | Dato           |

**Tabla 2. Inventario de activos**

El detallado de los activos por procesos y por actividades se encuentra en el Anexo 2.



### 3. Valorización de los activos de información

El siguiente paso a la identificación de los activos que se encuentren comprendidos dentro de los procesos “core” del instituto educativo es valorizarlos, y así determinar el valor que cada activo tiene para la organización y el impacto que tendría dentro de la misma si llegara a fallar en algún momento.

Para realizar dicha valorización, se determinó una escala cualitativa ya que no es posible valorar económicamente todos los activos envueltos dentro de estos procesos. En la siguiente tabla se muestra cuáles son los criterios que se usaron para realizar la correcta valorización de estos activos, en conjunto con los valores que se tendrán en cuenta para clasificarlos y su respectivo significado dentro del contexto actual:

| Criterio         | Valor | Descripción  |
|------------------|-------|--|
| Disponibilidad   | 0     | No Aplica / No es relevante  |
|                  | 1     | Debe estar disponible al menos el 10% del tiempo   |
|                  | 2     | Debe estar disponible al menos el 50% del tiempo   |
|                  | 3     | Debe estar disponible siempre  |
| Integridad       | 0     | No Aplica / No es relevante  |
|                  | 1     | No es relevante los errores que tenga o la información faltante                                      |
|                  | 2     | Tiene que estar correcto y completo al menos en un 50%   |
|                  | 3     | Tiene que estar correcto y completo en un 100%   |
| Confidencialidad | 0     | No Aplica / No es relevante  |
|                  | 1     | Daños muy bajos, el incidente no trascendería del área afectada                                      |
|                  | 2     | Sería relevantes, el incidente implicaría a otras áreas  |
|                  | 3     | Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas |

**Tabla 2. Criterios de valorización de activos**

Para hallar el valor final del activo, se realizará una suma de los valores de los distintos criterios. Esta suma se ubicará en el rango de valores de 0 a 9, para lo cual cada valor representara a un nivel de criticidad. Mientras más alto sea el número

final que resulto de la suma, más alta será su criticidad. Para este proyecto, se definieron cuatro niveles de criticidad del activo: no aplica, bajo, medio y alto.

A continuación, la siguiente tabla detalla el universo de valores que se puede obtener, asociados a un nivel de criticidad específico.

| Valor | Criticidad |
|-------|------------|
| 0     | No Aplica  |
| 1     | Baja       |
| 2     | Baja       |
| 3     | Baja       |
| 4     | Medio      |
| 5     | Medio      |
| 6     | Medio      |
| 7     | Alta       |
| 8     | Alta       |
| 9     | Alta       |

**Tabla 3. Valores según nivel de criticidad**

### **Apetito del riesgo**

Se definió que los activos cuya criticidad sea “Alta” son los que entrarán dentro de la identificación y análisis de riesgos de los activos de información del siguiente capítulo. Los activos con criticidad “Media” y “Baja” no se toman como activos críticos para la organización, por lo cual no entrarán dentro de dicho análisis.

Luego de haber definido el contexto de la valorización, se procederá a mostrar el total de los activos identificados con el valor respectivo que cada activo tiene dentro de la organización:

| Valorización de los activos |  |   |                |                  |             |             |
|-----------------------------|--|---|----------------|------------------|-------------|-------------|
| ID                          | Activo   | Criterios de valorización (ver pestaña Criterios) |                |                  | Valor total | Critricidad |
|                             |  | Integridad  | Disponibilidad | Confidencialidad |             |             |
| 1                           | Computadora de escritorio                        | 3   | 3              | 3                | 9           | Alta        |
| 2                           | Licencia de Microsoft Windows XP                 | 3   | 3              | 1                | 7           | Alta        |
| 3                           | Licencia de Microsoft Office 2007                | 3   | 3              | 1                | 7           | Alta        |
| 4                           | Página web del Instituto Educativo               | 2   | 3              | 2                | 7           | Alta        |
| 5                           | Intranet de la institución                       | 3   | 2              | 3                | 8           | Alta        |
| 6                           | Email (para el envío electrónico de información) | 2   | 3              | 3                | 8           | Alta        |
| 7                           | Teléfono   | 3   | 3              | 0                | 6           | Medio       |
| 8                           | Impresora  | 3   | 2              | 0                | 5           | Medio       |
| 9                           | Fotocopiadora                                    | 3   | 2              | 0                | 5           | Medio       |
| 10                          | Scanner  | 3   | 1              | 0                | 4           | Medio       |
| 11                          | Cableado Ethernet                                | 3   | 3              | 2                | 8           | Alta        |
| 12                          | Red del instituto (carpetas compartidas)         | 3   | 2              | 3                | 8           | Alta        |
| 13                          | Firewall   | 2   | 3              | 1                | 6           | Medio       |
| 14                          | Aula   | 2   | 3              | 0                | 5           | Medio       |
| 15                          | Vitrinas informativas                            | 1   | 1              | 0                | 2           | Baja        |
| 16                          | Oficina de reuniones                             | 2   | 2              | 2                | 6           | Medio       |
| 17                          | Sistema de información SMART                     | 3   | 3              | 3                | 9           | Alta        |
| 18                          | Servidor para el sistema de información SMART    | 3   | 3              | 3                | 9           | Alta        |
| 19                          | Archivadores para los documentos                 | 2   | 1              | 2                | 5           | Medio       |
| 20                          | Archivos de la sede                              | 3   | 3              | 3                | 9           | Alta        |
| 21                          | Gabinetes  | 2   | 1              | 2                | 5           | Medio       |
| 22                          | Llaves de ingreso                                | 3   | 3              | 3                | 9           | Alta        |

| Valorización de los activos |  |   |                    |                      |             |             |
|-----------------------------|--|---|--------------------|----------------------|-------------|-------------|
| ID                          | Activo   | Criterios de valorización (ver pestaña Criterios) |                    |                      | Valor total | Critricidad |
|                             |  | Integridad  | Disponibilida<br>d | Confidencialida<br>d |             |             |
| 23                          | Director Académico   | 3   | 0                  | 0                    | 3           | Baja        |
| 24                          | Stakeholder interno  | 3   | 2                  | 0                    | 5           | Medio       |
| 25                          | Stakeholder externo  | 3   | 2                  | 0                    | 5           | Medio       |
| 26                          | Gerente de Sede  | 3   | 2                  | 0                    | 5           | Medio       |
| 27                          | Jefe de Secretaría Académica   | 3   | 2                  | 0                    | 5           | Medio       |
| 28                          | Analista de procesos   | 3   | 0                  | 0                    | 3           | Baja        |
| 29                          | Director de Operaciones  | 3   | 2                  | 0                    | 5           | Medio       |
| 30                          | Director Comercial   | 3   | 2                  | 0                    | 5           | Medio       |
| 31                          | Jefe Académico   | 3   | 2                  | 0                    | 5           | Medio       |
| 32                          | Asistente de Programación  | 3   | 2                  | 0                    | 5           | Medio       |
| 33                          | Facilitador  | 3   | 2                  | 0                    | 5           | Medio       |
| 34                          | Jefe de Servicios Educativos   | 3   | 2                  | 0                    | 5           | Medio       |
| 35                          | Jefe Comercial   | 3   | 2                  | 0                    | 5           | Medio       |
| 36                          | Telemarketer / Promotor de Ventas  | 3   | 2                  | 0                    | 5           | Medio       |
| 37                          | Cliente  | 3   | 2                  | 0                    | 5           | Medio       |
| 38                          | Alumno   | 3   | 2                  | 0                    | 5           | Medio       |
| 39                          | Cajero   | 3   | 2                  | 0                    | 5           | Medio       |
| 40                          | Asistente Administrativo   | 3   | 2                  | 0                    | 5           | Medio       |
| 41                          | Calígrafo  | 3   | 2                  | 0                    | 5           | Medio       |
| 42                          | Egresado   | 3   | 2                  | 0                    | 5           | Medio       |
| 43                          | Asistente de Admisión  | 3   | 2                  | 0                    | 5           | Medio       |
| 44                          | Asistente Académico  | 3   | 2                  | 0                    | 5           | Medio       |
| 45                          | Jefe de Coordinación   | 3   | 2                  | 0                    | 5           | Medio       |
| 46                          | Servidor web   | 3   | 3                  | 3                    | 9           | Alta        |
| 47                          | Documento del perfil profesional de la nueva carrera (misión, perfil del egresado, etc.) | 2   | 1                  | 3                    | 6           | Medio       |
| 48                          | Documento del nuevo plan de estudios   | 3   | 1                  | 3                    | 7           | Alta        |

| Valorización de los activos |   |   |                    |                      |             |             |
|-----------------------------|---|---|--------------------|----------------------|-------------|-------------|
| ID                          | Activo  | Criterios de valorización (ver pestaña Criterios) |                    |                      | Valor total | Critricidad |
|                             |   | Integridad  | Disponibilida<br>d | Confidencialida<br>d |             |             |
| 49                          | Información estratégica del instituto                                 | 3   | 1                  | 3                    | 7           | Alta        |
| 50                          | Documento de información del análisis del mercado                     | 3   | 1                  | 1                    | 5           | Medio       |
| 51                          | Acta formal de constitución   | 1   | 1                  | 3                    | 5           | Medio       |
| 52                          | Documento de encuestas  | 1   | 1                  | 1                    | 3           | Baja        |
| 53                          | Documentos estadísticos del mercado educativo                         | 2   | 1                  | 2                    | 5           | Medio       |
| 54                          | Informe con el resultado de la investigación                          | 3   | 2                  | 2                    | 7           | Alta        |
| 55                          | Acta del comité consultivo  | 2   | 1                  | 1                    | 4           | Medio       |
| 56                          | Documento de la proyección anual de la oferta educativa (presupuesto) | 2   | 1                  | 2                    | 5           | Medio       |
| 57                          | Documento de la programación académica anual y mensual                | 3   | 2                  | 3                    | 8           | Alta        |
| 58                          | Reporte de alumnos aptos para matricularse                            | 3   | 2                  | 3                    | 8           | Alta        |
| 59                          | Información de alumnos de semestres anteriores                        | 3   | 2                  | 3                    | 8           | Alta        |
| 60                          | Impreso de la programación de frecuencias                             | 3   | 1                  | 1                    | 5           | Medio       |
| 61                          | Plan semestral/anual de cursos a dictarse                             | 3   | 2                  | 1                    | 6           | Medio       |
| 62                          | Evaluación 360°   | 2   | 1                  | 1                    | 4           | Medio       |
| 63                          | Evaluación del Jefe Académico   | 2   | 1                  | 1                    | 4           | Medio       |
| 64                          | Encuesta académica  | 1   | 1                  | 1                    | 3           | Baja        |
| 65                          | Registro de información del facilitador                               | 3   | 1                  | 2                    | 6           | Medio       |
| 66                          | Documento de programación tentativa de facilitadores                  | 3   | 2                  | 1                    | 6           | Medio       |
| 67                          | Documento de programación de facilitadores                            | 3   | 2                  | 1                    | 6           | Medio       |
| 68                          | Materiales de estudio (silabo, presentaciones, casos, lecturas)       | 2   | 2                  | 1                    | 5           | Medio       |
| 69                          | Información sobre la evaluación de la "Evaluación 360°"               | 3   | 1                  | 1                    | 5           | Medio       |
| 70                          | Resultado de calificaciones de la "Evaluación 360°"                   | 3   | 1                  | 2                    | 6           | Medio       |
| 71                          | Registro de aulas   | 1   | 2                  | 1                    | 4           | Medio       |
| 72                          | Documento de frecuencia de cursos por campaña                         | 3   | 2                  | 2                    | 7           | Alta        |
| 73                          | Documento de alumnos inscritos por campaña                            | 3   | 2                  | 3                    | 8           | Alta        |
| 74                          | Documento de la programación de las aulas                             | 2   | 2                  | 1                    | 5           | Medio       |

| Valorización de los activos |   |   |                    |                      |             |             |
|-----------------------------|---|---|--------------------|----------------------|-------------|-------------|
| ID                          | Activo  | Criterios de valorización (ver pestaña Criterios) |                    |                      | Valor total | Critricidad |
|                             |   | Integridad  | Disponibilida<br>d | Confidencialida<br>d |             |             |
| 75                          | Base de datos de potenciales clientes                             | 3   | 3                  | 3                    | 9           | Alta        |
| 76                          | Servidor para la base de datos de potenciales clientes            | 3   | 3                  | 3                    | 9           | Alta        |
| 77                          | Informe de resultados de llamadas a clientes                      | 3   | 2                  | 2                    | 7           | Alta        |
| 78                          | Información sobre preferencias de los clientes                    | 3   | 2                  | 3                    | 8           | Alta        |
| 79                          | Guión de comunicación e información de productos                  | 2   | 3                  | 0                    | 5           | Medio       |
| 80                          | Material informativo / Documentación relacionada a los programas  | 2   | 3                  | 0                    | 5           | Medio       |
| 81                          | Brochure del programa   | 3   | 3                  | 0                    | 6           | Medio       |
| 82                          | Reglamento de admisión  | 3   | 2                  | 1                    | 6           | Medio       |
| 83                          | Formulario de Preinscripción                                      | 3   | 3                  | 1                    | 7           | Alta        |
| 84                          | Ficha de Admisión   | 3   | 3                  | 1                    | 7           | Alta        |
| 85                          | Registro de orden de cobro a los clientes inscritos               | 3   | 2                  | 3                    | 8           | Alta        |
| 86                          | Consolidado de la información de las fichas de admisión (virtual) | 3   | 2                  | 2                    | 7           | Alta        |
| 87                          | Evaluación de Aptitud Emprendedora (Examen de admisión)           | 3   | 2                  | 1                    | 6           | Medio       |
| 88                          | Resultados de la Evaluación de Aptitud Emprendedora               | 3   | 3                  | 3                    | 9           | Alta        |
| 89                          | Certificado original de estudios de 1° a 5° de secundaria         | 3   | 0                  | 3                    | 6           | Medio       |
| 90                          | Partida de nacimiento original (o copia legalizada)               | 3   | 0                  | 3                    | 6           | Medio       |
| 91                          | Fotocopia de DNI  | 3   | 0                  | 3                    | 6           | Medio       |
| 92                          | Voucher de pago de Admisión                                       | 3   | 0                  | 3                    | 6           | Medio       |
| 93                          | Ficha de Admisión (en físico)                                     | 3   | 3                  | 2                    | 8           | Alta        |
| 94                          | Ficha de Matricula (en físico)                                    | 3   | 3                  | 2                    | 8           | Alta        |
| 95                          | Reporte de alumnos matriculados (en físico)                       | 3   | 2                  | 2                    | 7           | Alta        |
| 96                          | Ficha de preinscripción de matrícula                              | 3   | 3                  | 1                    | 7           | Alta        |
| 97                          | Consolidación bancaria (vía email)                                | 3   | 3                  | 3                    | 9           | Alta        |
| 98                          | Voucher de pago de matrícula                                      | 3   | 2                  | 1                    | 6           | Medio       |
| 99                          | Registro de las matriculas  | 3   | 2                  | 1                    | 6           | Medio       |
| 100                         | Solicitud o cartas de descuento                                   | 3   | 1                  | 1                    | 5           | Medio       |

| Valorización de los activos |   |   |                |                  |             |            |
|-----------------------------|---|---|----------------|------------------|-------------|------------|
| ID                          | Activo  | Criterios de valorización (ver pestaña Criterios) |                |                  | Valor total | Criticidad |
|                             |   | Integridad  | Disponibilidad | Confidencialidad |             |            |
| 101                         | Reporte visado de cartas de descuento         | 3   | 2              | 2                | 7           | Alta       |
| 102                         | Solicitud de expedición del título            | 2   | 2              | 1                | 5           | Medio      |
| 103                         | Ficha de inscripción para la titulación       | 2   | 3              | 1                | 6           | Medio      |
| 104                         | Declaración jurada del egresado               | 3   | 1              | 1                | 5           | Medio      |
| 105                         | Certificado de estudios superiores (original) | 3   | 2              | 3                | 8           | Alta       |
| 106                         | Foto  | 3   | 2              | 3                | 8           | Alta       |
| 107                         | Recibo de pago por derecho de titulación      | 3   | 2              | 2                | 7           | Alta       |
| 108                         | Acta visada por la DRE                        | 3   | 2              | 3                | 8           | Alta       |
| 109                         | Formato del Ministerio de Trabajo             | 2   | 1              | 0                | 3           | Baja       |
| 110                         | Diploma                                       | 3   | 2              | 3                | 8           | Alta       |
| 111                         | Acta de sustentación de tesis                 | 2   | 2              | 1                | 5           | Medio      |
| 112                         | Título de egresado                            | 3   | 2              | 3                | 8           | Alta       |
| 113                         | Fotocopia del título de egresado              | 2   | 2              | 3                | 7           | Alta       |

Tabla 4. Valorización de los activos



## Capítulo 3: Identificación y Evaluación de los Riesgos

### 1. Mapa de Riesgos

Previamente al desarrollo del mapa de riesgos se procedió a realizar una valorización detallada de riesgos, los cuales involucran hallar las vulnerabilidades y amenazas que puedan afectar a los activos que se ubican dentro del apetito de riesgo previamente definido.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. Finalmente, se optó por la realización de una matriz de calor, la cual tiene como criterios la probabilidad que cierta amenaza explote cierta vulnerabilidad y el impacto al negocio estimado que la ocurrencia del riesgo pueda ocasionar al negocio. A continuación se presenta la matriz de calor con los criterios que se han definido.

| Impacto en el Negocio | Probabilidad de Afectación |           |           |          |           |
|-----------------------|----------------------------|-----------|-----------|----------|-----------|
|                       | Muy Baja                   | Baja      | Media     | Alta     | Muy Alta  |
| Muy Alto              | Relevante                  | Relevante | Alto      | Crítico  | Crítico   |
| Alto                  | Relevante                  | Relevante | Alto      | Alto     | Crítico   |
| Medio                 | Moderado                   | Moderado  | Relevante | Alto     | Crítico   |
| Bajo                  | Bajo                       | Bajo      | Bajo      | Moderado | Relevante |
| Muy Bajo              | Bajo                       | Bajo      | Bajo      | Bajo     | Moderado  |

Tabla 5. Matriz de calor

Los significados de los cinco valores que los criterios de “Impacto en el Negocio” y “Probabilidad de Afectación” puedan tener son descritos a continuación.

Con respecto al criterio de “Probabilidad de Afectación”:

| Probabilidad de Afectación | Interpretación  |
|----------------------------|---|
| Muy Alta                   | Es casi seguro que la amenaza afectará la vulnerabilidad. |
| Alta                       | Es probable que la amenaza afectará la vulnerabilidad.    |
| Media                      | Es posible que la amenaza afectará la vulnerabilidad.     |
| Baja                       | Es improbable que la amenaza afectará la vulnerabilidad.  |
| Muy Baja                   | Es impensable que la amenaza afectará la vulnerabilidad.  |

Tabla 6. Descripción de los niveles de la Probabilidad de Afectación

Con respecto al criterio de “Impacto en el Negocio”:

| Impacto en el Negocio | Interpretación  |
|-----------------------|---|
| Muy Alto              | Afecta por más de una semana las operaciones del instituto. |
| Alto                  | Afecta hasta en 72 horas las operaciones del instituto.     |

| Impacto en el Negocio | Interpretación   |
|-----------------------|--|
| Medio                 | Afecta hasta en 24 horas las operaciones del instituto.                        |
| Bajo                  | Afecta hasta en 6 horas las operaciones del instituto.                         |
| Muy Bajo              | Tiene un efecto nulo o muy pequeño en las operaciones del instituto educativo. |

**Tabla 7. Descripción de los niveles de Impacto en el Negocio**

Luego de evaluar y definir la probabilidad y el impacto en el negocio que pueda ocasionar la materialización de los riesgos identificados obtenemos el nivel de dichos riesgos. Como se observa en el mapa de calor, se pudieron obtener cinco valores de riesgo: bajo, moderado, relevante, alto y crítico. En el siguiente capítulo, se establecerá un criterio de aceptación del riesgo, el cual servirá para realizar un plan de tratamiento de riesgo: si el riesgo es aceptable o si requiere algún tratamiento para reducir, evitar o transferir dicho riesgo.

A continuación se presenta la matriz completa de riesgos de los activos (críticos) que entraron en el análisis, según el apetito de riesgo establecido.

| Matriz de Riesgos |                                  |   |   |   |                                    |                 |
|-------------------|----------------------------------|---|---|---|------------------------------------|-----------------|
| ID de Riesgo      | Activo                           | Vulnerabilidad  | Amenaza   | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
| R1                | Computadora de escritorio        | Falta de cierre de sesión al momento de salir de la estación de trabajo | Manipulación de información                     | Alto  | Alto                               | Alto            |
| R2                | Computadora de escritorio        | Sensibilidad a la humedad, polvo y al calor                             | Polvo, corrosión, congelamiento                 | Medio   | Muy Alto                           | Alto            |
| R3                | Computadora de escritorio        | Susceptibilidad a variaciones en el voltaje                             | Perdida de suministro de energía                | Alto  | Muy Alto                           | Crítico         |
| R4                | Computadora de escritorio        | Sensibilidad de golpes o caídas   | Destrucción de equipos o medios de comunicación | Bajo  | Muy Alto                           | Relevante       |
| R5                | Computadora de escritorio        | Falta de backups de información   | Robo de información o del mismo equipo          | Muy Alto  | Muy Alto                           | Crítico         |
| R6                | Computadora de escritorio        | Mala seguridad de contraseñas   | Espionaje remoto                                | Alto  | Muy Alto                           | Crítico         |
| R7                | Licencia de Microsoft Windows XP | Falta de mecanismos de autenticación e identificación de usuarios       | Abuso o forzado de derechos                     | Bajo  | Muy Alto                           | Relevante       |

## Matriz de Riesgos

| ID de Riesgo | Activo   | Vulnerabilidad  | Amenaza                           | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
|--------------|--|---|-----------------------------------|---|------------------------------------|-----------------|
| R8           | Licencia de Microsoft Windows XP                 | Mala gestión de contraseñas                                       | Abuso o forzado de derechos       | Bajo  | Muy Alto                           | Relevante       |
| R9           | Licencia de Microsoft Windows XP                 | Servicios innecesarios para el usuario                            | Procesamiento ilegal de los datos | Alto  | Muy Alto                           | Crítico         |
| R10          | Licencia de Microsoft Office 2007                | Falta de mecanismos de autenticación e identificación de usuarios | Abuso o forzado de derechos       | Bajo  | Alto                               | Relevante       |
| R11          | Licencia de Microsoft Office 2007                | Mala gestión de contraseñas                                       | Abuso o forzado de derechos       | Bajo  | Alto                               | Relevante       |
| R12          | Licencia de Microsoft Office 2007                | Servicios innecesarios para el usuario                            | Procesamiento ilegal de los datos | Alto  | Alto                               | Alto            |
| R13          | Página web del Instituto Educativo               | Falta de pruebas del software                                     | Abuso de derechos                 | Medio   | Medio                              | Relevante       |
| R14          | Página web del Instituto Educativo               | Defectos en el funcionamiento del software                        | Abuso de derechos                 | Alto  | Medio                              | Alto            |
| R15          | Página web del Instituto Educativo               | Interfaz de usuario complicada                                    | Error en el uso del software      | Alto  | Medio                              | Alto            |
| R16          | Página web del Instituto Educativo               | Falta de documentación  | Error en el uso del software      | Medio   | Medio                              | Relevante       |
| R17          | Página web del Instituto Educativo               | Servicios innecesarios para el usuario                            | Procesamiento ilegal de los datos | Alto  | Medio                              | Alto            |
| R18          | Intranet de la institución                       | Defectos en el funcionamiento del software                        | Abuso de derechos                 | Alto  | Alto                               | Alto            |
| R19          | Intranet de la institución                       | Pocos o nulos controles de acceso                                 | Abuso de derechos                 | Alto  | Alto                               | Alto            |
| R20          | Intranet de la institución                       | Interfaz de usuario complicada                                    | Error en el uso del software      | Alto  | Alto                               | Alto            |
| R21          | Intranet de la institución                       | Fechas incorrectas  | Error en el accionar              | Bajo  | Alto                               | Relevante       |
| R22          | Intranet de la institución                       | Mala gestión de contraseñas                                       | Abuso de derechos                 | Medio   | Alto                               | Alto            |
| R23          | Intranet de la institución                       | Servicios innecesarios para el usuario                            | Procesamiento ilegal de los datos | Alto  | Alto                               | Alto            |
| R24          | Email (para el envío electrónico de información) | Defectos en el funcionamiento del software                        | Abuso de derechos                 | Alto  | Alto                               | Alto            |
| R25          | Email (para el envío electrónico de información) | Falta de un log de pistas de auditoría                            | Abuso de derechos                 | Medio   | Alto                               | Alto            |
| R26          | Email (para el envío electrónico de información) | Fechas incorrectas  | Error en el accionar              | Muy Bajo  | Alto                               | Relevante       |

## Matriz de Riesgos

| ID de Riesgo | Activo   | Vulnerabilidad  | Amenaza                                      | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
|--------------|--|---|--|---|------------------------------------|-----------------|
| R27          | Email (para el envío electrónico de información) | Falta de mecanismos de autenticación e identificación de usuarios       | Abuso de derechos                            | Medio   | Alto                               | Alto            |
| R28          | Email (para el envío electrónico de información) | Falta de backups de información   | Manipulación de información                  | Medio   | Alto                               | Alto            |
| R29          | Cableado Ethernet                                | Trafico de información desprotegido                                     | Escuchar información ilegalmente             | Medio   | Alto                               | Alto            |
| R30          | Cableado Ethernet                                | Cableado desprotegido   | Falla en los equipos de comunicaciones       | Alto  | Alto                               | Alto            |
| R31          | Cableado Ethernet                                | Arquitectura de red insegura  | Espionaje remoto                             | Bajo  | Alto                               | Relevante       |
| R32          | Cableado Ethernet                                | Gestión inadecuada de la red  | Saturación de los sistemas de información    | Alto  | Alto                               | Alto            |
| R33          | Red del instituto (carpetas compartidas)         | Falta de controles en el traspaso de información                        | Robo de documentos o de equipos tecnológicos | Alto  | Alto                               | Alto            |
| R34          | Red del instituto (carpetas compartidas)         | Falta de privilegios en los permisos                                    | Manipulación de información                  | Muy Alto  | Alto                               | Crítico         |
| R35          | Red del instituto (carpetas compartidas)         | Mala seguridad de contraseñas   | Manipulación de información                  | Alto  | Alto                               | Alto            |
| R36          | Red del instituto (carpetas compartidas)         | Gestión inadecuada de la red  | Saturación de los sistemas de información    | Alto  | Alto                               | Alto            |
| R37          | Red del instituto (carpetas compartidas)         | Conexiones de red desprotegidas   | Uso no autorizado de los equipos de red      | Medio   | Alto                               | Alto            |
| R38          | Sistema de información SMART                     | Defectos en el funcionamiento del software                              | Abuso de derechos                            | Medio   | Muy Alto                           | Alto            |
| R39          | Sistema de información SMART                     | Falta de cierre de sesión al momento de salir de la estación de trabajo | Manipulación de información                  | Alto  | Muy Alto                           | Crítico         |
| R40          | Sistema de información SMART                     | Falta de un log de pistas de auditoria                                  | Abuso de derechos                            | Medio   | Muy Alto                           | Alto            |
| R41          | Sistema de información SMART                     | Pocos o nulos controles de acceso                                       | Abuso de derechos                            | Alto  | Muy Alto                           | Crítico         |
| R42          | Sistema de información SMART                     | Interfaz de usuario complicada  | Error en el uso del software                 | Alto  | Muy Alto                           | Crítico         |
| R43          | Sistema de información SMART                     | Falta de documentación  | Error en el uso del software                 | Medio   | Muy Alto                           | Alto            |
| R44          | Sistema de información SMART                     | Fechas incorrectas  | Error en el accionar                         | Muy Bajo  | Muy Alto                           | Relevante       |
| R45          | Sistema de información SMART                     | Servicios innecesarios para el usuario                                  | Procesamiento ilegal de los datos            | Alto  | Muy Alto                           | Crítico         |
| R46          | Sistema de información SMART                     | Software nuevo o con fallas   | Mal funcionamiento del software              | Muy Alto  | Muy Alto                           | Crítico         |

## Matriz de Riesgos

| ID de Riesgo | Activo  | Vulnerabilidad   | Amenaza  | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
|--------------|---|--|--|---|------------------------------------|-----------------|
| R47          | Sistema de información SMART                  | Falta de backups de información  | Manipulación de información con software               | Medio   | Muy Alto                           | Alto            |
| R48          | Sistema de información SMART                  | Falta de mecanismos de backup  | Robo o pérdida de documentos                           | Alto  | Muy Alto                           | Crítico         |
| R49          | Servidor para el sistema de información SMART | Falta de una adecuada gestión de reemplazo o mantenimiento             | Destrucción de equipos o medios de comunicación        | Bajo  | Muy Alto                           | Relevante       |
| R50          | Servidor para el sistema de información SMART | Sensibilidad a la humedad, polvo y al calor                            | Polvo, corrosión, congelamiento                        | Medio   | Muy Alto                           | Alto            |
| R51          | Servidor para el sistema de información SMART | Sensibilidad a la radiación electromagnética                           | Radiación electromagnética                             | Muy Bajo  | Muy Alto                           | Relevante       |
| R52          | Servidor para el sistema de información SMART | Susceptibilidad a variaciones en el voltaje                            | Perdida de suministro de energía                       | Medio   | Muy Alto                           | Alto            |
| R53          | Servidor para el sistema de información SMART | Susceptibilidad a variaciones en la temperatura                        | Fenómenos meteorológicos                               | Muy Bajo  | Muy Alto                           | Relevante       |
| R54          | Servidor para el sistema de información SMART | Sensibilidad de golpes o caídas  | Destrucción de equipos o medios de comunicación        | Alto  | Muy Alto                           | Crítico         |
| R55          | Servidor para el sistema de información SMART | Falta de controles para acceder al ambiente del servidor               | Robo de documentos o de equipos tecnológicos           | Alto  | Muy Alto                           | Crítico         |
| R56          | Archivos de la sede                           | Falta de mecanismos de backup  | Robo o pérdida de documentos                           | Alto  | Muy Alto                           | Crítico         |
| R57          | Archivos de la sede                           | Falta de cuidado en el transporte o en su transferencia                | Robo o manipulación del activo                         | Alto  | Muy Alto                           | Crítico         |
| R58          | Llaves de ingreso                             | Uso inadecuado o sin cuidado de accesos a instalaciones o habitaciones | Destrucción o robo de equipos o medios de comunicación | Alto  | Muy Alto                           | Crítico         |
| R59          | Servidor web                                  | Falta de mecanismos de autenticación e identificación de usuarios      | Abuso de derechos                                      | Bajo  | Alto                               | Relevante       |
| R60          | Servidor web                                  | Mala gestión de contraseñas  | Abuso de derechos                                      | Muy Bajo  | Alto                               | Relevante       |
| R61          | Servidor web                                  | Servicios innecesarios para el usuario                                 | Procesamiento ilegal de los datos                      | Bajo  | Alto                               | Relevante       |
| R62          | Documento del nuevo plan de estudios          | Falta de mecanismos de backup  | Robo o pérdida de documentos                           | Bajo  | Muy Alto                           | Relevante       |
| R63          | Documento del nuevo plan de estudios          | Falta de cuidado en el transporte o en su transferencia                | Robo o manipulación del activo                         | Medio   | Muy Alto                           | Alto            |
| R64          | Documento del nuevo plan de estudios          | Pocos o nulos controles de acceso                                      | Robo o manipulación del activo                         | Alto  | Muy Alto                           | Crítico         |

| Matriz de Riesgos |  |   |                                |   |                                    |                 |
|-------------------|--|---|--------------------------------|---|------------------------------------|-----------------|
| ID de Riesgo      | Activo   | Vulnerabilidad  | Amenaza                        | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
| R65               | Informe con el resultado de la investigación           | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R66               | Informe con el resultado de la investigación           | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R67               | Informe con el resultado de la investigación           | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R68               | Documento de la programación académica anual y mensual | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R69               | Documento de la programación académica anual y mensual | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R70               | Documento de la programación académica anual y mensual | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R71               | Reporte de alumnos aptos para matricularse             | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R72               | Reporte de alumnos aptos para matricularse             | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R73               | Reporte de alumnos aptos para matricularse             | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R74               | Información de alumnos de semestres anteriores         | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Alto                               | Relevante       |
| R75               | Información de alumnos de semestres anteriores         | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Medio   | Alto                               | Alto            |
| R76               | Documento de frecuencia de cursos por campaña          | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R77               | Documento de frecuencia de cursos por campaña          | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R78               | Documento de frecuencia de cursos por campaña          | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R79               | Documento de alumnos inscritos por campaña             | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |



| Matriz de Riesgos |   |   |                                |   |                                    |                 |
|-------------------|---|---|--------------------------------|---|------------------------------------|-----------------|
| ID de Riesgo      | Activo  | Vulnerabilidad  | Amenaza                        | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
| R80               | Documento de alumnos inscritos por campaña                        | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R81               | Documento de alumnos inscritos por campaña                        | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R82               | Formulario de Preinscripción                                      | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R83               | Formulario de Preinscripción                                      | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R84               | Ficha de Admisión   | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R85               | Ficha de Admisión   | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R86               | Registro de orden de cobro a los clientes inscritos               | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R87               | Registro de orden de cobro a los clientes inscritos               | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R88               | Registro de orden de cobro a los clientes inscritos               | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Muy Alto  | Alto                               | Crítico         |
| R89               | Consolidado de la información de las fichas de admisión (virtual) | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R90               | Consolidado de la información de las fichas de admisión (virtual) | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R91               | Consolidado de la información de las fichas de admisión (virtual) | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R92               | Resultados de la Evaluación de Aptitud Emprendedora               | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R93               | Resultados de la Evaluación de Aptitud Emprendedora               | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |

| Matriz de Riesgos |   |   |                                |   |                                    |                 |
|-------------------|---|---|--------------------------------|---|------------------------------------|-----------------|
| ID de Riesgo      | Activo  | Vulnerabilidad  | Amenaza                        | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
| R94               | Resultados de la Evaluación de Aptitud Emprendedora | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R95               | Ficha de Admisión (en físico)                       | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Muy Alto                           | Crítico         |
| R96               | Ficha de Admisión (en físico)                       | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R97               | Ficha de Matricula (en físico)                      | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R98               | Ficha de Matricula (en físico)                      | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R99               | Reporte de alumnos matriculados (en físico)         | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R100              | Reporte de alumnos matriculados (en físico)         | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R101              | Reporte de alumnos matriculados (en físico)         | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R102              | Ficha de preinscripción de matrícula                | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R103              | Ficha de preinscripción de matrícula                | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R104              | Reporte visado de cartas de descuento               | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R105              | Reporte visado de cartas de descuento               | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R106              | Certificado de estudios superiores (original)       | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R107              | Certificado de estudios superiores (original)       | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R108              | Certificado de estudios superiores (original)       | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R109              | Foto  | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R110              | Foto  | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |

| Matriz de Riesgos |  |   |                                |   |                                    |                 |
|-------------------|--|---|--------------------------------|---|------------------------------------|-----------------|
| ID de Riesgo      | Activo                                   | Vulnerabilidad  | Amenaza                        | Posibilidad de que la amenaza explote la vulnerabilidad | Impacto estimado en la institución | Nivel de Riesgo |
| R111              | Foto                                     | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R112              | Recibo de pago por derecho de titulación | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Muy Alto  | Alto                               | Crítico         |
| R113              | Recibo de pago por derecho de titulación | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Bajo  | Alto                               | Relevante       |
| R114              | Acta visada por la DRE                   | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R115              | Acta visada por la DRE                   | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R116              | Acta visada por la DRE                   | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R117              | Diploma                                  | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R118              | Diploma                                  | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R119              | Diploma                                  | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R120              | Título de egresado                       | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R121              | Título de egresado                       | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R122              | Título de egresado                       | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |
| R123              | Fotocopia del título de egresado         | Falta de mecanismos de backup                           | Robo o pérdida de documentos   | Bajo  | Muy Alto                           | Relevante       |
| R124              | Fotocopia del título de egresado         | Falta de cuidado en el transporte o en su transferencia | Robo o manipulación del activo | Medio   | Muy Alto                           | Alto            |
| R125              | Fotocopia del título de egresado         | Pocos o nulos controles de acceso                       | Robo o manipulación del activo | Alto  | Muy Alto                           | Crítico         |

Tabla 8. Matriz de riesgos

## 2. Plan de tratamiento de riesgos

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su integridad, confidencialidad o disponibilidad; se definió un criterio de aceptación del riesgo el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. Finalmente, se obtiene el plan de tratamiento de los riesgos identificados previamente.

A continuación se presenta el plan de tratamiento de los riesgos:

| Nivel de Riesgo | Política para la toma de Acciones |
|-----------------|-----------------------------------|
| Crítico         | Riesgo no aceptable               |
| Alto            | Riesgo no deseable                |
| Relevante       | Riesgo aceptable                  |
| Moderado        | Riesgo aceptable                  |
| Bajo            | Riesgo aceptable                  |

**Tabla 9. Plan de tratamiento de riesgos**

El tratamiento de los riesgos cuyo nivel sea “Crítico” o “Alto” es recurrir a la implementación de ciertos controles para reducir la probabilidad que dichos riesgos identificados se materialicen. Finalmente, no se requerirá de tratamiento para los niveles de riesgos de “Relevante”, “Moderado” y “Bajo” ya que se considera que la institución educativa puede convivir con dichos riesgos.

## 3. Controles para el tratamiento de riesgos

Los controles que se han seleccionado para el tratamiento de los riesgos son los que se detallan en el estándar ISO 27002, el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general. Cabe resaltar que dichos controles siguen lineamientos generales, en la Declaración de la Aplicabilidad se mostrarán los controles adaptados a la realidad organizacional del instituto educativo estudiado.

Para empezar se definió controles respecto a las políticas de seguridad que la institución busca establecer para alcanzar el nivel de seguridad deseado. Cabe resaltar que todos estos controles o políticas contribuyen a la mitigación de todos los riesgos identificados y, en su mayoría, deberán ser desarrollados y promovidos por la Alta Gerencia de la entidad educativa.

Estos controles y políticas de seguridad son los siguientes:

| Clausula                                       | Categoría de Seguridad               | Nombre Control  | Descripción  |
|--|--------------------------------------|---|--|
| Política de seguridad                          | Política de seguridad de información | Documentar política de seguridad de información                         | La alta gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.   |
|  |                                      | Revisión de la política de seguridad de la información                  | La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.  |
| Organización de la seguridad de la información | Organización interna                 | Compromiso de la gerencia con la seguridad de la información            | La alta gerencia de debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. |
|  |                                      | Coordinación de la seguridad de información                             | Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.  |
|  |                                      | Asignación de responsabilidades de la seguridad de la información       | Se deben definir claramente las responsabilidades de la seguridad de la información.   |
|  |                                      | Proceso de autorización para los medios de procesamiento de información | Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información.   |
|  |                                      | Acuerdos de confidencialidad  | Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.                                      |
|  | Entidades externas                   | Tratamiento de la seguridad cuando se trabaja con clientes              | Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.  |
| Gestión de activos                             | Responsabilidad por los activos      | Inventarios de activos  | Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.   |

| Clausula  | Categoría de Seguridad   | Nombre Control  | Descripción   |
|---|--|---|---|
|   | Clasificación de la información                                    | Uso aceptable de los activos                                    | Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.  |
|   |  | Lineamientos de clasificación                                   | La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.   |
|   |  | Etiquetado y manejo de la información                           | Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.   |
| Gestión de incidentes en la seguridad de la información | Reporte de eventos y debilidades en la seguridad de la información | Reporte de eventos en la seguridad de la información            | Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.  |
|   |  | Reporte de debilidades en la seguridad                          | Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.   |
|   | Gestión de incidentes y mejoras en la seguridad de la información  | Responsabilidades y procedimientos                              | Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.   |
|   |  | Aprendizaje de los incidentes en la seguridad de la información | Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.  |
|   |  | Recolección de evidencia  | Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes. |
| Cumplimiento  | Cumplimiento con requerimientos legales                            | Protección los registros organizacionales                       | Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.   |
|   |  | Protección de data y privacidad de información personal         | Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.   |

| Clausula   | Categoría de Seguridad                            | Nombre Control  | Descripción   |
|--|---|---|---|
|  |   | Prevención de mal uso de medios de procesamiento de información | Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.              |
| Gestión de las comunicaciones y operaciones                            | Procedimientos y responsabilidades operacionales  | Procedimientos de operación documentados                        | Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten. |
| Control de acceso  | Gestión del acceso del usuario                    | Revisión de los derechos de acceso del usuario                  | La alta gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.               |
| Adquisición, desarrollo y mantenimiento de los sistemas de información | Seguridad en los procesos de desarrollo y soporte | Desarrollo de outsource software                                | El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.                                |

**Tabla 10. Políticas de seguridad**

Luego de definir las políticas de seguridad que la organización deberá adoptar, se procede a listar los controles para el tratamiento de los diversos riesgos identificados; especificando el control, su descripción según la norma ISO 27002, los riesgos que mitigará y la adaptación de dicho control con la realidad organizacional de la institución educativa.

| Clausula                     | Categoría de Seguridad | Nombre Control                               | Descripción   | Riesgos a Controlar | Adaptación a la entidad educativa   |
|------------------------------|------------------------|--|---|---------------------|---|
| Seguridad física y ambiental | Áreas seguras          | Controles de entrada físicos                 | Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado. | R55, R58            | Se deberán proteger las áreas seguras del instituto mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado. |
|                              |                        | Seguridad de oficinas, habitaciones y medios | Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.  | R55, R58            | Se deberán diseñar y aplicar controles de seguridad físicos en las oficinas, habitaciones y medios.   |



| Clausula                                    | Categoría de Seguridad                              | Nombre Control                      | Descripción  | Riesgos a Controlar                    | Adaptación a la entidad educativa  |
|---|---|-------------------------------------|--|--|--|
|   | Seguridad del equipo                                | Ubicación y protección del equipo   | El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.  | R2, R50, R52, R55                      | Los equipos electrónicos críticos deberán estar ubicados de tal manera que ayudarán a reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.  |
|   |   | Servicios públicos                  | El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.  | R2, R3, R50, R52                       | Los equipos electrónicos críticos deberán ser protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios eléctricos o de telecomunicaciones   |
|   |   | Seguridad en el cableado            | El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la interceptación o daño.  | R3, R29, R30, R32, R52                 | El cableado eléctrico y de las telecomunicaciones que llevan data o sostienen los servicios de información del instituto deberán ser protegidos mediante tubos u otros controles   |
|   |   | Mantenimiento de equipo             | El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.  | R2, R3, R50, R52, R14,                 | Los equipos deberán pasar por mantenimiento 1 vez mensual para asegurar la continuidad de los sistemas y demás aplicativos que dan soporte a los procesos críticos   |
| Gestión de las comunicaciones y operaciones | Planeación y aceptación del sistema                 | Aceptación del sistema              | Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación. | R14, R15, R18, R20, R24, R38, R42, R46 | Los gerentes del instituto deberán asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deberán pasar a producción luego de obtener la aceptación formal. |
|   | Protección contra software malicioso y código móvil | Controles contra software malicioso | Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos.  | R14, R18, R24, R38                     | La protección contra códigos maliciosos se deberá basar en la detección de códigos maliciosos dentro de los sistemas del instituto y la reparación del software, conciencia de seguridad, y los apropiados controles de acceso a los sistemas.   |

| Clausula | Categoría de Seguridad        | Nombre Control                                       | Descripción   | Riesgos a Controlar  | Adaptación a la entidad educativa   |
|----------|-------------------------------|--|---|--|---|
|          | Respaldo (back-up)            | Back-up o respaldo de la información                 | Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.   | R82, R84, R86, R95, R97, R102, R104, R112                              | La institución educativa deberá proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y crítica se pueda recuperar después de algún desastre o falla de medios.  |
|          | Gestión de seguridad de redes | Controles de red                                     | Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.                         | R29, R30, R32, R36, R37  | El área de Sistemas de la institución deberá implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.  |
|          | Gestión de medios             | Procedimientos de manejo de la información           | Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.   | R69, R72, R77, R80, R90, R93, R100, R107, R110, R115, R118, R121, R124 | Se deberán establecer procedimientos para la manipulación, procesamiento, almacenamiento y comunicación de la información consistente con su clasificación  |
|          | Intercambio de información    | Procedimientos y políticas de información y software | Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.   | R69, R72, R77, R80, R90, R93, R100, R107, R110, R115, R118, R121, R124 | Se deberán establecer políticas, procedimientos y controles para proteger el intercambio de información que se dé en la sede del instituto a través de todos los tipos de medios de comunicación que se manejen (teléfonos, correo electrónico, etc.).                |
|          |                               | Mensajes electrónicos                                | Se debe proteger adecuadamente los mensajes electrónicos.   | R24, R27   | La institución deberá manejar distintas políticas y controles que le permitan manejar de manera segura el intercambio de información vía Email.   |
|          | Monitoreo                     | Registro de auditoría                                | Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso. | R25, R40   | La institución deberá producir logs de auditoría, excepciones y eventos de seguridad de información. Estos registros se deben mantener durante un periodo determinado para ayudar en investigaciones futuras y monitorear los sistemas y aplicativos que se necesiten |

| Clausula          | Categoría de Seguridad                 | Nombre Control                  | Descripción  | Riesgos a Controlar  | Adaptación a la entidad educativa   |
|-------------------|--|---------------------------------|--|--|---|
|                   |  | Uso del sistema de monitoreo    | Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente. | R25, R40   | La institución deberá determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo. La institución deberá cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo. |
| Control de acceso | Gestión del acceso del usuario         | Inscripción del usuario         | Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.                                      | R9, R12, R17, R19, R23, R27, R34, R41, R45, R64, R67, R70, R73, R75, R78, R81, R88, R91, R94, R101, R108, R111, R116, R119, R122, R125 | La institución deberá manejar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a los usuarios de todos los sistemas y servicios de información que la institución posea.   |
|                   |  | Gestión de privilegios          | Se debe restringir y controlar la asignación y uso de los privilegios.   | R9, R17, R23, R27, R34, R45  | Los sistemas multi-usuario del instituto que requieren protección contra el acceso no autorizado deberán controlar la asignación de privilegios a través de un proceso de autorización formal.  |
|                   |  | Gestión de la clave del usuario | La asignación de claves se debe controlar a través de un proceso de gestión formal.  | R6, R22, R35   | El área de Sistemas deberá proporcionar directrices para la gestión para las contraseñas de los distintos sistemas de información que se posean. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.                       |
|                   | Control de acceso al sistema operativo | Sistema de gestión de claves    | Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.   | R6, R22, R35   | El área de Sistemas deberá proporcionar políticas para las contraseñas de sesiones de Windows de los colaboradores con acceso a una PC. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.                                |

| Clausula | Categoría de Seguridad        | Nombre Control                            | Descripción   | Riesgos a Controlar | Adaptación a la entidad educativa   |
|----------|-------------------------------|---|---|---------------------|---|
|          | Responsabilidades del usuario | Uso de clave                              | Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.  | R6, R22, R35        | El área de Sistemas deberá proporcionar políticas para las contraseñas de los distintos sistemas de información que se posean. Estas políticas deberán seguir buenas prácticas de seguridad en la selección y uso de claves.                                    |
|          | Responsabilidades del usuario | Equipo de usuario desatendido             | Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido  | R1, R39             | Todos los usuarios del instituto deberán estar al tanto de los requerimientos de seguridad y los procedimientos para proteger su respectivo equipo desatendido, así como sus responsabilidades para implementar dicha protección                                |
|          |                               | Política de pantalla y escritorio limpio  | Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información. | R1, R5              | La políticas de escritorio limpio y pantalla limpia que la alta dirección proporcione deberá tomar en cuenta las clasificaciones de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización |
|          | Control de acceso a redes     | Política sobre el uso de servicios en red | Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.   | R37                 | Se deberá formular una política relacionada con el uso de las redes y los servicios de la red, de tal manera que los usuarios del instituto sólo deberán tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.              |

| Clausula   | Categoría de Seguridad                           | Nombre Control   | Descripción  | Riesgos a Controlar    | Adaptación a la entidad educativa  |
|--|--|--|--|------------------------|--|
|  | Control de acceso al sistema operativo           | Identificación y autenticación del usuario                   | Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario. | R5, R6                 | Todos los usuarios de los sistemas del instituto deberán tener un identificador singular (ID de usuario) para su uso personal y exclusivo (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos) para poder verificar la identidad de la persona que acceda a la PC. |
|  |  | Uso de utilidades del sistema                                | Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.   | R9, R12, R17, R23, R45 | Se restringirá y controlará estrictamente el uso de los programas de utilidad que podrían ser capaces de superar los controles de Windows y de las aplicaciones a las cuales el usuario tiene acceso.  |
|  |  | Sesión inactiva  | Las sesiones inactivas deben cerrarse después de un período de inactividad definido.   | R1, R39                | Las sesiones inactivas de los usuarios de Windows deberán cerrarse después de un período de inactividad definido por el área de Sistemas.  |
|  | Control de acceso a la aplicación de información | Aislamiento del sistema sensible                             | Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).  | R50, R52, R54, R55     | Los sistemas críticos deberán tener un ambiente de cómputo dedicado (aislado) respecto a los demás sistemas que la institución educativa maneje. Esta área seguirá otro lineamiento de seguridad (por su nivel de criticidad).   |
| Adquisición, desarrollo y mantenimiento de los sistemas de información | Requerimientos de seguridad de los sistemas      | Análisis y especificación de los requerimientos de seguridad | Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.                             | R41, R45, R46, R48     | Los requerimientos de seguridad deberán ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.  |

Tabla 11. Controles para el tratamiento de riesgos

#### 4. Mapeo de los controles con COBIT 5

En este punto se identificarán los objetivos corporativos que COBIT 5 propone, relacionados a los objetivos de negocio del instituto educativo. Luego, se procederá a relacionar las metas de TI asociadas a dichos objetivos organizacionales y, a continuación, se identificará los procesos habilitadores que dan soporte al cumplimiento de dichas metas de TI. Todo este mapeo sigue el esquema de la “Cascada de Objetivos” que propone COBIT 5 (figura 10). Finalmente, se comparará y evaluará los procesos habilitadores finales con los controles para el tratamiento de los riesgos que se establecieron en el punto anterior.

Cabe recordar que COBIT 5 se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer. Asimismo, la audiencia objetivo es la alta gerencia, en conjunto con los demás gerentes de las demás áreas. Mientras que los controles que propone la ISO 27002, tienen un mayor grado de detalle, siendo enfocados a la parte de la implementación de dichos controles dentro de la organización. Habiendo dado una mayor luz al enfoque de cada marco y/o norma, se procede a realizar el mapeo correspondiente.

Los objetivos organizacionales que propone COBIT 5 y que la organización desea lograr son:

| Dimensión BSC | N° | Metas de la organización                                    |
|---------------|----|---|
| Financiero    | 1  | Retorno de valor de las inversiones de los Stakeholders     |
| Financiero    | 2  | Portafolio competitivo de los productos y servicios         |
| Financiero    | 3  | Riesgos de negocio gestionados (Salvaguarda de los activos) |
| Financiero    | 4  | Cumplimiento de las leyes y reglamentos externos            |
| Cliente       | 6  | Cultura de servicio orientada al cliente                    |
| Cliente       | 7  | Continuidad y disponibilidad del servicio                   |
| Cliente       | 8  | Respuesta ágil a los cambios en el entorno empresarial      |
| Cliente       | 9  | Información basada en toma de decisiones estratégicas       |
| Interno       | 11 | Optimización de la funcionalidad de los procesos de negocio |
| Interno       | 12 | Optimización de los costos de los procesos de negocio       |
| Interno       | 14 | Productividad de las operaciones y el personal              |

| Dimensión BSC             | N° | Metas de la organización                         |
|---------------------------|----|--|
| Interno                   | 15 | Cumplimiento de las políticas internas           |
| Aprendizaje y Crecimiento | 16 | Personas cualificadas y motivadas                |
| Aprendizaje y Crecimiento | 17 | Cultura de innovación de productos y del negocio |

**Tabla 12. Objetivos organizacionales de la entidad educativa según COBIT 5**

A continuación, en la tabla siguiente podemos apreciar la relación de los objetivos de TI requeridos para el logro de los objetivos organizacionales mencionados en la tabla anterior. La lista completa de los objetivos de TI propuestos por COBIT 5 se ubica en el anexo 3.

| ID | Objetivos del Instituto Educativo de Nivel Superior     | ID TI | Objetivos de TI   |
|----|---|-------|---|
| 1  | Retorno de valor de las inversiones de los Stakeholders | 1     | Alineación de las TI y las estrategias del negocio  |
|    |   | 3     | Compromiso de la alta dirección para hacer decisiones relacionadas con TI   |
|    |   | 5     | Beneficios logrados de inversiones en TI y en el portafolio de servicios  |
|    |   | 7     | Servicios de TI alineados con los requerimientos del negocio  |
|    |   | 11    | Optimización de los activos, recursos y capacidades de TI   |
| 2  | Portafolio competitivo de los productos y servicios     | 13    | Entrega de programas entregando beneficios a tiempo y en el presupuesto cumpliendo con los requisitos y estándares de calidad |
|    |   | 1     | Alineación de las TI y las estrategias del negocio  |
|    |   | 5     | Beneficios logrados de inversiones en TI y en el portafolio de servicios  |
|    |   | 7     | Servicios de TI alineados con los requerimientos del negocio  |
|    |   | 9     | Agilidad de TI  |
|    |   | 12    | Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en los mismos                          |



| ID | Objetivos del Instituto Educativo de Nivel Superior         | ID TI | Objetivos de TI  |
|----|---|-------|--|
|    |   | 17    | Conocimiento, experiencia e iniciativas para la innovación empresarial       |
| 3  | Riesgos de negocio gestionados (Salvaguarda de los activos) | 4     | Gestión de riesgos del negocio relacionados con TI                           |
|    |   | 10    | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
|    |   | 16    | Personal de TI cualificado y motivado  |
| 4  | Cumplimiento de las leyes y reglamentos externos            | 2     | Apoyo de TI para el cumplimiento de las leyes y reglamentos externos         |
|    |   | 10    | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
| 6  | Cultura de servicio orientada al cliente                    | 1     | Alineación de las TI y las estrategias del negocio                           |
|    |   | 7     | Servicios de TI alineados con los requerimientos del negocio                 |
| 7  | Continuidad y disponibilidad del servicio                   | 1     | Alineación de las TI y las estrategias del negocio                           |
|    |   | 4     | Gestión de riesgos del negocio relacionados con TI                           |
|    |   | 10    | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
|    |   | 14    | Disponibilidad de información fiable y útil para la toma de decisiones       |
| 8  | Respuesta ágil a los cambios en el entorno empresarial      | 7     | Servicios de TI alineados con los requerimientos del negocio                 |
|    |   | 9     | Agilidad de TI   |
|    |   | 17    | Conocimiento, experiencia e iniciativas para la innovación empresarial       |
| 9  | Información basada en toma de decisiones estratégicas       | 1     | Alineación de las TI y las estrategias del negocio                           |
|    |   | 14    | Disponibilidad de información fiable y útil para la toma de decisiones       |
| 10 | Optimización de los costos de prestación de servicios       | 4     | Gestión de riesgos del negocio relacionados con TI                           |
|    |   | 6     | Transparencia de los costos, beneficios y riesgos de TI                      |
|    |   | 11    | Optimización de los activos, recursos y capacidades de TI                    |
| 11 | Optimización de la funcionalidad de los procesos de negocio | 1     | Alineación de las TI y las estrategias del negocio                           |
|    |   | 7     | Servicios de TI alineados con los requerimientos del negocio                 |

| ID | Objetivos del Instituto Educativo de Nivel Superior   | ID TI | Objetivos de TI  |
|----|---|-------|--|
|    |   | 8     | Uso adecuado de las aplicaciones, información y soluciones tecnológicas                              |
|    |   | 9     | Agilidad de TI   |
|    |   | 12    | Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en los mismos |
| 12 | Optimización de los costos de los procesos de negocio | 5     | Beneficios logrados de inversiones en TI y en el portafolio de servicios                             |
|    |   | 6     | Transparencia de los costos, beneficios y riesgos de TI  |
|    |   | 11    | Optimización de los activos, recursos y capacidades de TI  |
| 14 | Productividad de las operaciones y el personal        | 8     | Uso adecuado de las aplicaciones, información y soluciones tecnológicas                              |
|    |   | 16    | Personal de TI cualificado y motivado  |
| 15 | Cumplimiento de las políticas internas                | 2     | Apoyo de TI para el cumplimiento de las leyes y reglamentos externos                                 |
|    |   | 10    | Seguridad de la información, infraestructura de procesamiento y aplicaciones                         |
|    |   | 15    | Cumplimiento de TI con las políticas internas  |
| 16 | Personas cualificadas y motivadas                     | 16    | Personal de TI cualificado y motivado  |
| 17 | Cultura de innovación de productos y del negocio      | 9     | Agilidad de TI   |
|    |   | 17    | Conocimiento, experiencia e iniciativas para la innovación empresarial                               |

**Tabla 13. Objetivos de TI de la entidad educativa según los objetivos organizacionales**

Siguiendo con el mapeo, en la siguiente tabla se procede a relacionar los objetivos de TI con los procesos habilitadores que COBIT 5 define. Cabe resaltar que estos procesos habilitadores dan soporte a la realización y logro de dichos objetivos.

| ID TI | Objetivos de TI   | ID Proc. | Procesos habilitadores  |
|-------|---|----------|---|
| 1     | Alineación de las TI y las estrategias del negocio                        | BAI02    | Gestionar la definición de requisitos                           |
|       |   | EDM01    | Asegurar el mantenimiento y ajuste del marco de gobierno        |
| 2     | Apoyo de TI para el cumplimiento de las leyes y reglamentos externos      | APO12    | Gestionar riesgos   |
|       |   | BAI10    | Gestionar la configuración                                      |
|       |   | MEA02    | Monitorear y evaluar el sistema de control interno              |
|       |   | MEA03    | Monitorear y evaluar el cumplimiento de requerimientos externos |
| 3     | Compromiso de la alta dirección para hacer decisiones relacionadas con TI | EDM01    | Asegurar el mantenimiento y ajuste del marco de gobierno        |
|       |   | EDM05    | Garantizar la transparencia de los stakeholders                 |
| 4     | Gestión de riesgos del negocio relacionados con TI                        | APO10    | Administrar Proveedores   |
|       |   | APO12    | Gestionar riesgos   |
|       |   | BAI06    | Gestionar los cambios   |
|       |   | DSS03    | Gestión de problemas  |
|       |   | DSS06    | Administrar los controles de procesos del negocio               |
|       |   | MEA01    | Monitorear y evaluar el rendimiento y la conformidad            |
|       |   | MEA02    | Monitorear y evaluar el sistema de control interno              |
| 5     | Beneficios logrados de inversiones en TI y en el portafolio de servicios  | MEA03    | Monitorear y evaluar el cumplimiento de requerimientos externos |
|       |   | APO10    | Administrar Proveedores   |
| 6     | Transparencia de los costos, beneficios y riesgos de TI                   | APO12    | Gestionar riesgos   |
|       |   | BAI09    | Gestionar los activos   |
|       |   | EDM05    | Garantizar la transparencia de los stakeholders                 |
| 7     | Servicios de TI alineados con los requerimientos del negocio              | APO10    | Administrar Proveedores   |
|       |   | BAI02    | Gestionar la definición de requisitos                           |
|       |   | BAI06    | Gestionar los cambios   |
|       |   | DSS03    | Gestión de problemas  |
|       |   | DSS06    | Administrar los controles de procesos del negocio               |
|       |   | EDM01    | Asegurar el mantenimiento y ajuste del marco de gobierno        |
|       |   | EDM05    | Garantizar la transparencia de los stakeholders                 |
| 8     | Uso adecuado de las aplicaciones, información y soluciones tecnológicas   | MEA01    | Monitorear y evaluar el rendimiento y la conformidad            |
|       |   | BAI07    | Gestionar la transición y aceptación del cambio                 |
| 9     | Agilidad de TI  | APO10    | Administrar Proveedores   |

| ID TI | Objetivos de TI   | ID Proc. | Procesos habilitadores                               |
|-------|---|----------|--|
|       |   | BAI08    | Gestión del conocimiento                             |
| 10    | Seguridad de la información, infraestructura de procesamiento y aplicaciones  | APO12    | Gestionar riesgos                                    |
|       |   | BAI06    | Gestionar los cambios                                |
| 11    | Optimización de los activos, recursos y capacidades de TI   | BAI09    | Gestionar los activos                                |
|       |   | BAI10    | Gestionar la configuración                           |
|       |   | DSS03    | Gestión de problemas                                 |
|       |   | MEA01    | Monitorear y evaluar el rendimiento y la conformidad |
| 12    | Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en los mismos                          | BAI02    | Gestionar la definición de requisitos                |
|       |   | BAI07    | Gestionar la transición y aceptación del cambio      |
| 13    | Entrega de programas entregando beneficios a tiempo y en el presupuesto cumpliendo con los requisitos y estándares de calidad | APO12    | Gestionar riesgos                                    |
| 14    | Disponibilidad de información fiable y útil para la toma de decisiones  | BAI10    | Gestionar la configuración                           |
|       |   | DSS03    | Gestión de problemas                                 |
| 15    | Cumplimiento de TI con las políticas internas   | MEA01    | Monitorear y evaluar el rendimiento y la conformidad |
|       |   | MEA02    | Monitorear y evaluar el sistema de control interno   |
| 16    | Personal de TI cualificado y motivado   | APO12    | Gestionar riesgos                                    |
| 17    | Conocimiento, experiencia e iniciativas para la innovación empresarial  | BAI08    | Gestión del conocimiento                             |

**Tabla 14. Procesos habilitadores de COBIT 5 según los objetivos de TI de la entidad educativa**

Finalmente, se presenta la tabla con el detalle del mapeo entre los procesos habilitadores identificados y los controles establecidos en el punto anterior para el tratamiento de los riesgos de los activos en la institución.

| ID    | Proceso Habilitador     | ID Control | Nombre Control               | Descripción   |
|-------|-------------------------|------------|------------------------------|---|
| APO10 | Administrar Proveedores | A.6.1.5    | Acuerdos de confidencialidad | Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información. |

| ID    | Proceso Habilitador                             | ID Control | Nombre Control  | Descripción  |
|-------|---|------------|---|--|
|       |   | A.12.5.5   | Desarrollo de software por terceros                                     | El desarrollo de software que ha sido tercerizado debe ser supervisado y monitoreado por la organización.  |
|       |   | A.15.1.4   | Protección de data y privacidad de información personal                 | Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.  |
| APO12 | Gestionar riesgos                               | A.13.1.1   | Reporte de eventos en la seguridad de la información                    | Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.   |
|       |   | A.13.1.2   | Reporte de debilidades en la seguridad                                  | Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.        |
| BAI02 | Gestionar la definición de requisitos           | A.10.1.1   | Procedimientos de operación documentados                                | Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.  |
|       |   | A.10.3.2   | Aceptación del sistema  | Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación. |
|       |   | A.11.6.2   | Aislamiento del sistema sensible  | Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).  |
|       |   | A.12.1.1   | Análisis y especificación de los requerimientos de seguridad            | Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.   |
| BAI06 | Gestionar los cambios                           | A.11.5.4   | Uso de utilidades del sistema   | Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.   |
| BAI07 | Gestionar la transición y aceptación del cambio | A.6.1.4    | Proceso de autorización para los medios de procesamiento de información | Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información  |

| ID    | Proceso Habilitador        | ID Control | Nombre Control  | Descripción  |
|-------|----------------------------|------------|---|--|
|       |                            | A.10.3.2   | Aceptación del sistema  | Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación. |
| BAI08 | Gestión del conocimiento   | A.10.1.1   | Procedimientos de operación documentados                        | Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.  |
|       |                            | A.10.3.2   | Aceptación del sistema  | Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación. |
|       |                            | A.13.2.2   | Aprendizaje de los incidentes en la seguridad de la información | Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.   |
| BAI09 | Gestionar los activos      | A.7.1.1    | Inventarios de activos  | Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.  |
|       |                            | A.7.2.2    | Etiquetado y manejo de la información                           | Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.  |
|       |                            | A.15.1.5   | Prevención de mal uso de medios de procesamiento de información | Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.   |
| BAI10 | Gestionar la configuración | A.7.1.1    | Inventarios de activos  | Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.  |
|       |                            | A.7.2.2    | Etiquetado y manejo de la información                           | Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.  |

| ID    | Proceso Habilitador                                      | ID Control | Nombre Control  | Descripción   |
|-------|--|------------|---|---|
|       |  | A.15.1.5   | Prevención de mal uso de medios de procesamiento de información | Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.  |
| DSS03 | Gestión de problemas                                     | A.13.2.2   | Aprendizaje de los incidentes en la seguridad de la información | Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.  |
| DSS06 | Administrar los controles de procesos del negocio        | A.10.5.1   | Back-up o respaldo de la información                            | Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.   |
|       |  | A.10.6.1   | Controles de red  | Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.                       |
|       |  | A.10.7.3   | Procedimientos de manejo de la información                      | Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.   |
|       |  | A.10.8.4   | Mensajes electrónicos   | Se debe proteger adecuadamente los mensajes electrónicos.   |
| EDM01 | Asegurar el mantenimiento y ajuste del marco de gobierno | A.6.1.1    | Compromiso de la gerencia con la seguridad de la información    | La alta gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. |
| EDM05 | Garantizar la transparencia de los stakeholders          | A.6.1.1    | Compromiso de la gerencia con la seguridad de la información    | La alta gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. |
|       |  | A.6.1.2    | Coordinación de la seguridad de información                     | Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.   |



| ID    | Proceso Habilitador                                  | ID Control | Nombre Control  | Descripción   |
|-------|--|------------|---|---|
|       |  | A.6.1.3    | Asignación de responsabilidades de la seguridad de la información       | Se deben definir claramente las responsabilidades de la seguridad de la información.  |
|       |  | A.6.1.4    | Proceso de autorización para los medios de procesamiento de información | Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información   |
|       |  | A.6.1.5    | Acuerdos de confidencialidad  | Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información. |
| MEA01 | Monitorear y evaluar el rendimiento y la conformidad | A.5.1.2    | Revisión de la política de seguridad de la información                  | La alta gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.  |
|       |  | A.10.10.2  | Uso del sistema de monitoreo  | Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.                    |
| MEA02 | Monitorear y evaluar el sistema de control interno   | A.5.1.1    | Documentar política de seguridad de información                         | La alta gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.  |
|       |  | A.5.1.2    | Revisión de la política de seguridad de la información                  | La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.     |
|       |  | A.10.10.2  | Uso del sistema de monitoreo  | Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.                    |

| ID    | Proceso Habilitador   | ID Control | Nombre Control  | Descripción   |
|-------|---|------------|---|---|
| MEA03 | Monitorear y evaluar el cumplimiento de requerimientos externos | A.15.1.4   | Protección de data y privacidad de información personal | Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales. |

**Tabla 15. Procesos habilitadores de COBIT 5 para la entidad educativa**



## Capítulo 4: Entregables de un SGSI

### 1. Declaración de la Aplicabilidad

| Nombre Control                               | Adaptación al instituto educativo   | Riesgos a Controlar | Aplica? | Justificación  |
|--|---|---------------------|---------|--|
| Controles de entrada físicos                 | Se deberán proteger las áreas seguras de la institución mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.                                   | R55, R58            | Si      | Actualmente la entidad educativa toma en cuenta la protección de las distintas áreas que posee con algunos controles. Sin embargo, estos no son los adecuados conforme a las nuevas políticas de seguridad de información propuestas |
| Seguridad de oficinas, habitaciones y medios | Se deberán diseñar y aplicar controles de seguridad físicos en las oficinas, habitaciones y medios.   | R55, R58            | Si      | El instituto educativo toma en consideración las recomendaciones por parte de Defensa Civil con respecto a la seguridad en aulas y en otros ambientes físicos  |
| Ubicación y protección del equipo            | Los equipos electrónicos críticos deberán estar ubicados de tal manera que ayudarán a reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado. | R2, R50, R52, R55   | Si      | Si bien la institución tiene algunas políticas para la seguridad de los equipos electrónicos, estas no son las más adecuadas. Estas se ajustarán con respecto al nivel de seguridad deseado por la misma organización.               |

| Nombre Control                       | Adaptación al instituto educativo  | Riesgos a Controlar                       | Aplica? | Justificación   |
|--------------------------------------|--|---|---------|---|
| Servicios públicos                   | Los equipos electrónicos críticos deberán ser protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios eléctricos o de telecomunicaciones   | R2, R3, R50, R52                          | Si      | La institución educativa no posee algún control con respecto a las fallas de energía pero sabe de la criticidad de dichos controles   |
| Seguridad en el cableado             | El cableado eléctrico y de las telecomunicaciones que llevan data o sostienen los servicios de información de la institución deberán ser protegidos mediante tubos u otros controles   | R3, R29, R30, R32, R52                    | No      | Los gastos a invertir en una reestructuración del cableado de energía en toda la sede del instituto se incrementarían, excediendo lo planeado para la implantación de los controles                         |
| Mantenimiento de equipo              | Los equipos deberán pasar por mantenimiento 1 vez mensual para asegurar la continuidad de los sistemas y demás aplicativos que dan soporte a los procesos críticos   | R2, R3, R50, R52, R14,                    | Si      | La entidad educativa aún no posee políticas sobre el mantenimiento de los equipos, sino que el mantenimiento es bajo demanda  |
| Aceptación del sistema               | Los gerentes de la institución deberán asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deberán pasar a producción luego de obtener la aceptación formal. | R14, R15, R18, R20, R24, R38, R42, R46    | Si      | Este es un control que la Alta Dirección desea implantar. Previamente han tenido varios problemas con la falta de pruebas en los sistemas desarrollados internamente  |
| Controles contra software malicioso  | La protección contra códigos maliciosos se deberá basar en la detección de códigos maliciosos dentro de los sistemas de la institución y la reparación del software, conciencia de seguridad, y los apropiados controles de acceso a los sistemas.   | R14, R18, R24, R38                        | Si      | Adicionalmente a la falta de pruebas, es necesario implementar controles para la detección y prevención de ataques maliciosos a los sistemas.   |
| Back-up o respaldo de la información | El instituto educativo deberá proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y crítica se pueda recuperar después de algún desastre o falla de medios.   | R82, R84, R86, R95, R97, R102, R104, R112 | Si      | La institución tiene actualmente políticas de respaldo de información, sin embargo estas no son las más adecuadas. Estas se ajustarán con respecto al nivel de seguridad deseado por la misma organización. |

| Nombre Control                                       | Adaptación al instituto educativo   | Riesgos a Controlar  | Aplica? | Justificación  |
|--|---|--|---------|--|
| Controles de red                                     | El área de Sistemas del instituto educativo deberá implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.  | R29, R30, R32, R36, R37  | Si      | La seguridad de la arquitectura de Red del instituto es crítica para el instituto ya que manejan varios sistemas interconectados.  |
| Procedimientos de manejo de la información           | Se deberán establecer procedimientos para la manipulación, procesamiento, almacenamiento y comunicación de la información consistente con su clasificación  | R69, R72, R77, R80, R90, R93, R100, R107, R110, R115, R118, R121, R124 | Si      | Este control se relaciona directamente a las políticas de seguridad de información que la institución implementará.  |
| Procedimientos y políticas de información y software | Se deberán establecer políticas, procedimientos y controles para proteger el intercambio de información que se dé en la sede de la institución a través de todos los tipos de medios de comunicación que se maneje (teléfonos, correo electrónico, etc.).                     | R69, R72, R77, R80, R90, R93, R100, R107, R110, R115, R118, R121, R124 | Si      | Este control se relaciona directamente a las políticas de seguridad de información que la institución implementará.  |
| Mensajes electrónicos                                | El instituto educativo deberá manejar distintas políticas y controles que le permitan manejar de manera segura el intercambio de información vía Email.   | R24, R27   | Si      | Aun no se tiene ningún control con respecto al correo electrónico. Sin embargo, se deberá considerar ya que el mayor flujo de información entre los colaboradores del instituto se da a través de esta vía.            |
| Registro de auditoria                                | El instituto educativo deberá producir logs de auditoría, excepciones y eventos de seguridad de información. Estos registros se deben mantener durante un período determinado para ayudar en investigaciones futuras y monitorear los sistemas y aplicativos que se necesiten | R25, R40   | Si      | Si bien es cierto que aún no se posee con mecanismos de monitoreo y registro de acciones para auditorias, es algo necesario a implementar si es que se quiere lograr el nivel de seguridad deseado por la institución. |
| Uso del sistema de monitoreo                         | El instituto educativo deberá determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo. Asimismo, deberá cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo.                    | R25, R40   | No      | La compra e implantación de un sistema de monitoreo no está dentro de las prioridades de la institución. Este control puede implementarse en el futuro.  |

| Nombre Control                  | Adaptación al instituto educativo   | Riesgos a Controlar  | Aplica? | Justificación   |
|---------------------------------|---|--|---------|---|
| Inscripción del usuario         | La institución educativa deberá manejar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a los usuarios de todos los sistemas y servicios de información que posea.  | R9, R12, R17, R19, R23, R27, R34, R41, R45, R64, R67, R70, R73, R75, R78, R81, R88, R91, R94, R101, R108, R111, R116, R119, R122, R125 | Si      | EL instituto educativo maneja procedimientos para la asignación y eliminación de usuarios dentro de sus sistemas de información, sin embargo estos no son los más adecuados. Se ajustarán con respecto al nivel de seguridad deseado por la misma organización. |
| Gestión de privilegios          | Los sistemas multi-usuario de la institución que requieren protección contra el acceso no autorizado deberán controlar la asignación de privilegios a través de un proceso de autorización formal.  | R9, R17, R23, R27, R34, R45  | Si      | La institución maneja procedimientos para la asignación de accesos y privilegios dentro de los sistemas de información, sin embargo estos no son los más adecuados. Se ajustarán con respecto al nivel de seguridad deseado por la misma organización.          |
| Gestión de la clave del usuario | El área de Sistemas deberá proporcionar directrices para la gestión para las contraseñas de los distintos sistemas de información que el instituto posea. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.      | R6, R22, R35   | Si      | La institución gestiona las contraseñas dentro de los sistemas de información que posee, sin embargo no hay políticas formales. Estas se crearán para mantener un estándar en todos los sistemas.   |
| Sistema de gestión de claves    | El área de Sistemas deberá proporcionar políticas para las contraseñas de sesiones de Windows de los colaboradores con acceso a una PC. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.                        | R6, R22, R35   | Si      | El área de Sistemas ya maneja políticas para la gestión de contraseñas de los usuarios que tengan acceso a una PC y a Windows. Sin embargo, estas se ajustaran para lograr una mayor seguridad en Windows.  |
| Uso de clave                    | El área de Sistemas deberá proporcionar políticas para las contraseñas de los distintos sistemas de información que el instituto educativo posea. Estas políticas deberán seguir buenas prácticas de seguridad en la selección y uso de claves. | R6, R22, R35   | Si      | El área de Sistemas ya maneja políticas para la gestión de contraseñas de los usuarios que tengan acceso a una PC y a Windows. Sin embargo, estas se ajustaran para lograr una mayor seguridad en Windows.  |

| Nombre Control                             | Adaptación al instituto educativo  | Riesgos a Controlar    | Aplica? | Justificación   |
|--|--|------------------------|---------|---|
| Equipo de usuario desatendido              | Todos los usuarios del instituto educativo deberán estar al tanto de los requerimientos de seguridad y los procedimientos para proteger su respectivo equipo desatendido, así como sus responsabilidades para implementar dicha protección   | R1, R39                | Si      | Dentro de las políticas de seguridad que se implantarán, esta es una que la institución considera importante ya que hasta la fecha no se ha podido implantar una concientización en seguridad en los mismos usuarios. |
| Política de pantalla y escritorio limpio   | La políticas de escritorio limpio y pantalla limpia que la alta dirección proporcione deberá tomar en cuenta las clasificaciones de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización  | R1, R5                 | Si      | Dentro de las políticas de seguridad que se implantarán, esta es una que la institución considera importante ya que hasta la fecha no se ha podido implantar una concientización en seguridad en los mismos usuarios. |
| Política sobre el uso de servicios en red  | Se deberá formular una política relacionada con el uso de las redes y los servicios de la red, de tal manera que los usuarios del instituto sólo deberán tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.   | R37                    | Si      | En conjunto con las políticas de accesos a los sistemas y siguiendo las políticas de seguridad de información, la institución buscara formular una política para el uso de redes y servicios de red.                  |
| Identificación y autenticación del usuario | Todos los usuarios de los sistemas del instituto educativo deberán tener un identificador singular (ID de usuario) para su uso personal y exclusivo (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos) para poder verificar la identidad de la persona que acceda a la PC. | R5, R6                 | Si      | Al igual que se busca manejar adecuadamente la gestión de usuarios dentro de los sistemas del instituto educativo, también se busca gestionar la autenticación de los usuarios de Windows.                            |
| Uso de utilidades del sistema              | Se restringirá y controlará estrictamente el uso de los programas de utilidad que podrían ser capaces de superar los controles de Windows y de las aplicaciones a las cuales el usuario tiene acceso.  | R9, R12, R17, R23, R45 | Si      | Sigue la política de accesos de usuarios que la organización piensa implantar.  |



| Nombre Control   | Adaptación al instituto educativo   | Riesgos a Controlar | Aplica? | Justificación  |
|--|---|---------------------|---------|--|
| Sesión inactiva  | Las sesiones inactivas de los usuarios de Windows deberán cerrarse después de un periodo de inactividad definido por el área de Sistemas.   | R1, R39             | Si      | La institución aún no posee un auto-deslogeio del sistema pero es algo que el área de Sistemas piensa implantar para aumentar la seguridad   |
| Aislamiento del sistema sensible                             | Los sistemas críticos para la institución deberán tener un ambiente de cómputo dedicado (aislado) respecto a los demás sistemas que se manejen. Esta área seguirá otro lineamiento de seguridad (por su nivel de criticidad).   | R50, R52, R54, R55  | Si      | Los equipos más críticos para la institución se ubican en el mismo ambiente que el resto de equipos y servidores. Sin embargo, se deberá cambiar de ambiente al servidor del sistema Smart por ser un sistema crítico para la institución. |
| Análisis y especificación de los requerimientos de seguridad | Los requerimientos de seguridad deberán ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación. | R41, R45, R46, R48  | Si      | La organización busca obtener mayor seguridad en los sistemas que adquieran o desarrollen es por esto de la implementación de dicho control.   |

**Tabla 15. Declaración de la Aplicabilidad**

## Capítulo 5: Conclusiones y recomendaciones

### 1. Conclusiones y observaciones

Dentro de lo expuesto con la presente tesis se puede concluir lo siguiente:

- En conjunto con las personas, la información es el activo más importante que tiene cualquier organización. La falta de controles y políticas enfocadas a su seguridad puede traer consecuencias graves para el cumplimiento de los objetivos de negocio e incluso, pérdidas más graves de lo que la organización supone.
- No hay un interés adecuado con respecto a la seguridad de información dentro de las instituciones educativas, partiendo desde la alta gerencia hasta los mismos departamentos de TI.
- Dicha falta de interés se muestra claramente en la falta de políticas, normas y controles dentro del instituto educativo y en la falta de concientización del personal del mismo con respecto a la seguridad de la información.
- Un Sistema de Gestión de Seguridad de Información (SGSI) establecido en una institución educativa se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para

garantizar el cumplimiento de los objetivos de TI y, en consecuencia, los objetivos organizacionales.

- Para poder identificar adecuadamente los activos con los que cuenta cualquier organización, es importante realizar un modelado de los procesos involucrados dentro del alcance del SGSI. Para lo cual, en la presente tesis, se procedió a diagramar los procesos “core” utilizando la notación BPMN (Business Process Modeling Notation), la cual muestra de manera clara y concisa el flujo de actividades que se realizan en cada proceso.

Conforme a las observaciones, si bien los controles ayudan a mitigar o reducir algún riesgo identificado, algunos de estos no aplican a la realidad del instituto educativo en particular por diversos factores. Estos factores son importantes que se detallen dentro de la justificación de la aplicabilidad de dichos controles, la cual se especifica dentro del documento de la Declaración de Aplicabilidad que es un entregable de la presente tesis.

Finalmente, cabe resaltar que si no se cuenta con el apoyo de la alta gerencia de la institución educativa, no se contara con el soporte necesario para lograr los objetivos del SGSI. Asimismo, si el personal de la organización no sigue las políticas y lineamientos propuestos por la alta gerencia siguiendo dicho SGSI, no se obtendrá el nivel adecuado de seguridad en los flujos de información de los distintos procesos del instituto educativo.

## 2. Recomendaciones

Algunas recomendaciones que son importantes seguir para el desarrollo e implementación del SGSI dentro de un instituto educativo de nivel superior son:

- Realizar campañas de concientización periódicas para el personal de la institución con respecto a la seguridad de información, de tal manera que todos los empleados de los diversos niveles jerárquicos existentes de la institución educativa, conozcan la importancia y las consecuencias de no seguir los lineamientos de seguridad en el día a día.
- Lograr establecer un rol de “Oficial de Seguridad de Información” dentro de la institución educativa para el monitoreo y cumplimiento de las políticas y controles establecidos por la alta gerencia. Este rol no implica la contratación de personal, sino que puede ser algún colaborador del departamento de Sistemas del instituto.
- Actualizar periódicamente el SGSI. El plazo recomendado es cada 2 años ya que este periodo implica la posible adquisición de nuevas tecnologías dentro del campus del instituto educativo, o la posible modificación de las actividades de los procesos “core”, teniendo como consecuencia el incremento o

decremento de activos de información. Esta actualización, la debe realizar la persona que tenga el rol de “Oficial de Seguridad de Información” dentro de la institución.

- Realizar ejercicios de escritorio para comprobar los controles establecidos dentro del SGSI. Por lo menos una vez al año se deberían realizar dichas pruebas.



## Bibliografía

AMPUERO CHANG, Carlos Enrique

- [1] 2011 *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros*. Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Consulta: 15 de abril del 2012.  
<<http://tesis.pucp.edu.pe/repositorio/handle/123456789/933>>

ALEXANDER SERVAT, Alberto

- [13] 2007 *Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005*. Primera edición. México: Alfaomega Grupo Editor.

CANO, Jeimy

- [17] 2011 “El Debido Cuidado en Seguridad de Información. Un Ejercicio de Virtudes para el Responsable de la Seguridad de Información.”. *ISACA Journal*. 2011, Volumen 2, pp. 1-8.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

- [2] 2002 *ISO/IEC Guide 73:2002 Risk management -- Vocabulary -- Guidelines for use in standards*. EEUU.
- [3] 2004a *ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management*. EEUU.
- [4] 2004b *ISO/IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management*. EEUU.
- [5] 2005a *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements*. EEUU.
- [6] 2005b *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management*. EEUU.
- [7] 2010 *ISO/IEC 27003:2010 Information technology - Security techniques - Information security management systems implementation guidance*. EEUU.

- [12] 2008 *ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management*.EEUU.

IT GOVERNANCE INSTITUTE

- [8] 2012 *COBIT 5*. Illinois, USA.

MINISTERIO DE EDUCACION DEL PERU

- [9] 2005 *Reglamento de la Gestión del Sistema Educativo*. 09 de mayo.

PELNEKAR, Charu

- [14] 2011 "Planning for and Implementing ISO 27001". *ISACA Journal*. 2011, Volumen 4, pp. 1-8.

QUAGLIATA, Karen

- [18] 2011 "Impact of Security Awareness. Training Components on Perceived Security Effectiveness".*ISACA Journal Online*. 2011, Volumen 4, pp. 1-6.

ROSS, Steven J.

- [15] 2010 "IS Security Matters?". *ISACA Journal*. 2010, Volumen 2, pp. 1-2.
- [16] 2011 "What is the Value of Security?". *ISACA Journal*. 2011, Volumen 2, pp. 1-2.

TUPIA ANTICONA, Manuel Francisco

- [10] 2011 *Gobierno de las tecnologías de información bajo la óptica de COBIT 4.1*.Primera edición. Lima : Tupia consultores y auditores S.A.C.

VILLENA AGUILAR, Moisés Antonio

- [11] 2006 *Sistema de gestión de seguridad de información para una institución financiera*. Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Consulta: 15 de abril del 2012.  
<<http://tesis.pucp.edu.pe/repositorio/handle/123456789/362>>